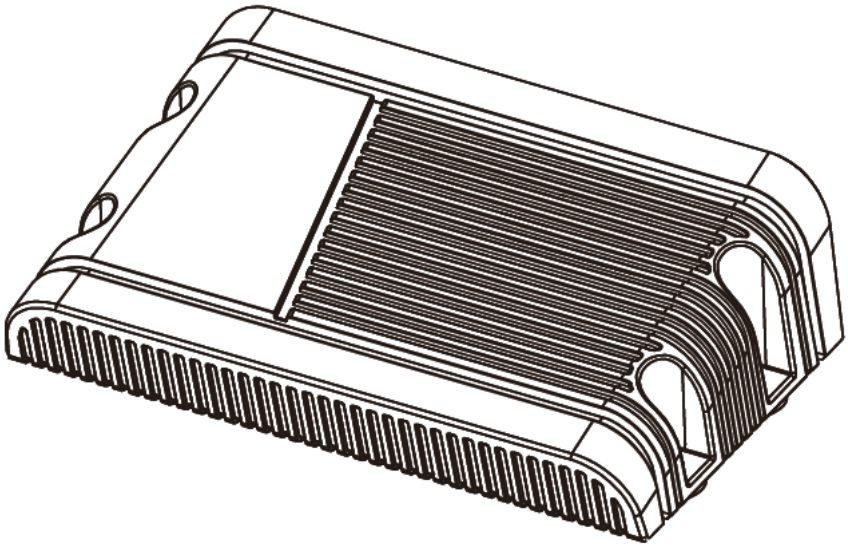
User Manual

BandLuxe

K530S

LTE M2M & Vehicle Mount Router



P/N:65018900011 Rev.A

BandLuxe™

Table of Contents

Package Contents 4
- Package Contents 4
- Optional Accessories 5
- Features 6
- Hardware Overview 6

Installation 8

Using Web-based Management 11
- Status 12
  - Overview 12
    - System 13
    - Network 13
    - DHCP Leases 13
    - Local Network 13
  - System Log 14
  - GPS 14
  - VnStat Traffic Monitor 14
    - Graphs 15
    - Configuration 15
  - Mobile Internet 16
    - Information 16
      - Signal Quality 16
      - U/SIM Status 16
      - Registered Network 17
      - Internet Connection 17
    - Debug 17
      - Debug 18
- System 19
  - System 19
    - System Properties 19
      - General Settings 19
      - Language and Style 20
    - Time Synchronization 20
    - Remote System Log 20
  - Administration 21
    - Router Password 21
    - Remote Access 21
  - Backup / Flash Firmware 22
    - Backup / Restore 22
      - Download backup 22
      - Reset to defaults 23
      - Restore backup 23
    - Flash new firmware image 23
    - Flash new module firmware image 23
    - Flash new ipkg package 23
  - Reboot 24
- Services 25
  - Dynamic DNS 25
  - Network Shares 26

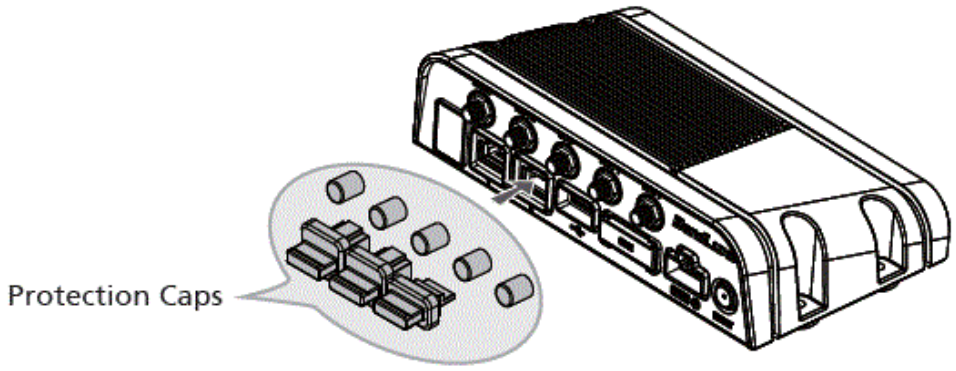
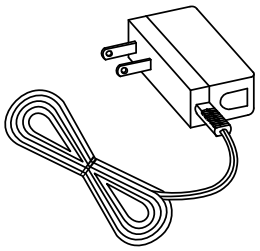
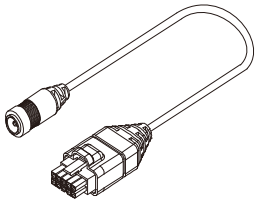
Samba 26
General Settings 26
Edit template 27
Shared Directories 27
Network 28
Interfaces 28
Interface Overview 28
Common Configuration 29
General Setup 29
Advanced Settings 29
Physical Settings 30
Firewall Settings 30
Hotspot 31
Chillispot 31
Mobile Internet 32
WWAN Setting 33
Network Settings 34
Reset Modem 34
Manually Update Phone Number 34
Manually Update MSID 34
Manually Update MIP Profile 34
eHRPD Menu 34
Enable LTE 34
U/SIM PIN Management 35
Scenario 1: No mobile internet service 35
Scenario 2: Mobile internet service pending 35
Scenario 3: Mobile internet service enabled 36
SIM Management 38
Preferred Network 38
AT command 39
Router 39
Router Settings 39
Router IP 39
DHCP Service 40
Active DHCP Leases 41
Static Leases 41
Advanced Routing settings 42
Static Routing 42
Routing and Redirection Service 43
VPN Passthrough 43
WiFi 44
Device Configuration 44
General Setup 44
Advanced Settings 46
Interface Configuration 46
General Setup 46
Wireless Security 47
MAC-Filter 51
Advanced Settings 51
Switch 52
Switch “eth0” (AR934X built-in switch) 52
VLAN on “eth0” (AR934X built-in switch) 52
Diagnostics 54
Network Utilities 54
Ping 54
Traceroute 54

NS Lookup 55
Firewall 56
Single Port Forward 56
Port Trigger 58
Security Filter 60
Firewall 60
Internet Filter 60
Web Filters 61
DMZ Host 61
IP Filtering 62
Port Range Forward 64
UPNP 66
UPnP Settings 66
VPN 66
IPSec Setting 66
IPSec VPN Connection 66
IPSec Profile 67
IPSec profile Overview 67
IPSec VPN connection status 67
IPSec Certificate 67
IPSec VPN Connection 67
SSL VPN 68
Help 69
Logout 69
Appendix A: Installation Guide for Vehicle Usage 70
Appendix B: FAQ 75
Appendix C: Specifications 82
Appendix D: Important Safety Information and Glossary 86
Europe – EU Declaration of Conformity 86
Federal Communication Commission Interference Statement 87
Glossary 89

Package Contents

Thank you for your purchase of this LTE M2M & Vehicle Mount Router. This product is designed to access the Internet via 4G technology and share the bandwidth through a Wi-Fi network. It is easy to configure and operate even for non-technical users. This manual contains instructions for installing and configuring the product. Read the manual carefully before you use the product, so that you can fully exploit the product functions.

Package Contents

<table>
<tr><td colspan="3"> 
</td></tr>
<tr><td colspan="3">BandLuxe LTE M2M & Vehicle Mount Router</td></tr>
<tr><td> </td><td>  </td><td>  </td></tr>
<tr><td>Mounting Screws</td><td>Power Adapter</td><td>Power Adapter Cable</td></tr>
</table>

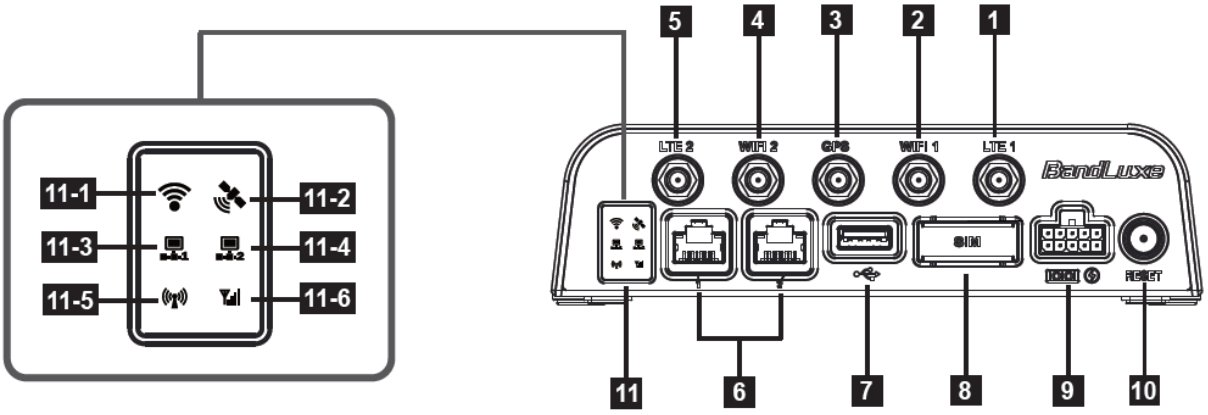
Optional Accessories

Water-Proof Magnetic BASE LTE Antenna	*Stick-type WiFi Antenna*
Water-Proof Active GPS Antenna	*Cigarette Lighter Power Converter*

Features

- LTE* Cat3 and 3GPP Rel9 compatible with HSPA+ or EVDO fallback support (*: LTE is a trademark of ETSI.)
- High performance module and router platform targeted for m2m and mission critical applications
- IP 64 and MIL 810G rugged design for extreme environments
- Operation temperature: -20°C to 70°C (-4°F to 158 °F)
- Input voltage: 12V or 24V DC, accepting 9-32V voltage swing
- 802.11 b/g/n 2x2 MIMO wireless networking
- Six status LEDs, two Ethernet ports, and one USB port
- IPSec VPN client and VPN pass-through modes
- Composite GPS and Glonass features for quicker positioning location and better accuracy

Hardware Overview



1	**4G External Antenna Port 1**	Connect the 4G External Antenna.
2	**WiFi 1**	Connect the WiFi External Antenna.
3	**GPS**	Connect the GPS External Antenna.
4	**WiFi 2**	Connect the second WiFi External Antenna. (Diversity antenna)

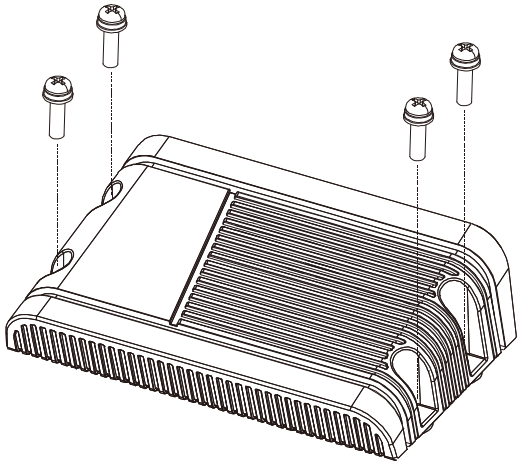
5	**4G External Antenna Port 2**	Connect the second 4G External Antenna. (Diversity antenna)		
6	**LAN Ports 1 and 2**	Connect the LAN device(s) as needed.		
7	**USB Port**	Connect the USB storage device.		
8	**SIM Card Tray Slot**	Insert the loaded SIM card tray for mobile internet connection.		
9	**Power Connector**	Connect the power adapter cable. K530 series router accepts 9~32V voltage swing.		
10	**Reset button**	Short press this button to reboot the router; Long press for 10 seconds to reset to factory default setting.		
11	**Network Status LEDs**			
11-1	**WiFi**	**Blue**	WiFi is on.	
11-2	**GPS**	**Blue**	GPS is on.	(Solid) Position is fixed. (Flashing) Position is not yet fixed.
11-3	**LAN1**	**Blue**	(Solid) LAN port is connected to PC or router. (Flashing) Data is be transmitted over LAN.	
11-4	**LAN2**	**Blue**		
11-5	**Network Status**	**Blue**	Under LTE network	(Solid) Connection is established. (Flashing) Connection is not yet established.
		Green	Under 3G network	
		Red	No signal, SIM error, Service failure, Invalid SIM.	
11-6	**Signal Strength**	**Blue**	Strong signal strength	
		Green	Good signal strengthl	
		Red	Weak signal strength or no signal	

[Note]

- When the device is in reboot, 4 LEDs (GPS, WiFi, LAN1, LAN2) will light up together.
- When the device is performing FW upgrade, GPS and WiFi LED will be flashing together.

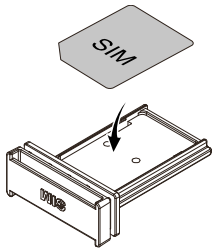
Installation

1. Mount the router with the four screws if needed.

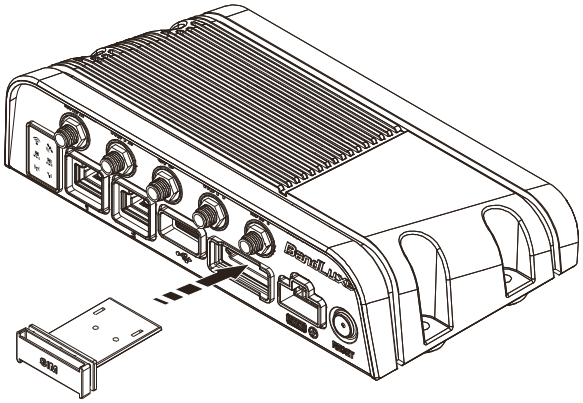


2. K530S has Sprint embedded SIM inside. For special application that you have to use an external SIM card, please follow below instruction to load the SIM card:

a) Place the SIM card tray upside down. Secure the SIM card (contact side up) onto the SIM card tray.

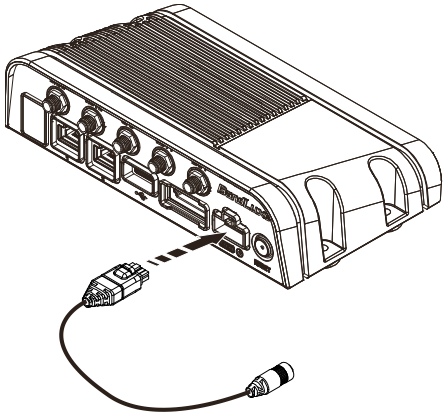


b) Insert your loaded SIM card tray into the slot on the router.

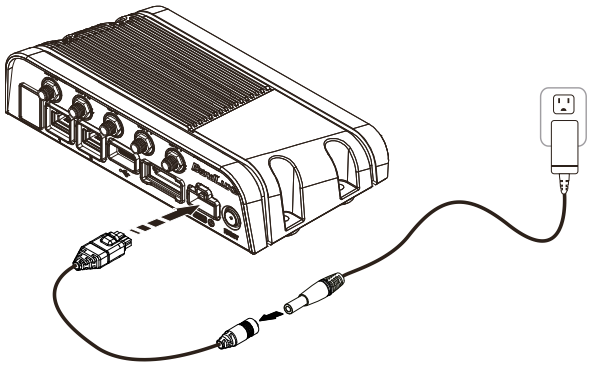


c) Once the external SIM is plug in, the embedded SIM will no longer be activated.

3. Connect the power adapter cable to the router.

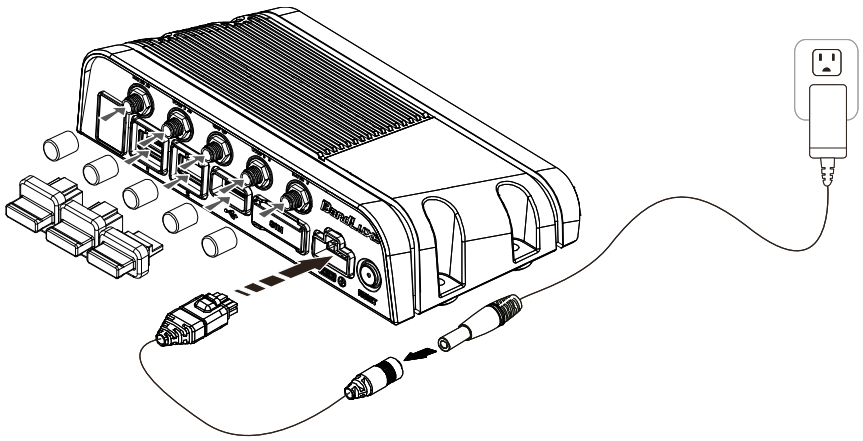


4. Connect the power adapter cable to either a power outlet (via the power adapter) or a 12/24V DC power source. The router will automatically be turned ON upon receiving power.



5. (Optional) For any of the antenna connectors to be connected to this router, remove the corresponding protective cap and connect the GPS antenna, the WiFi antenna, or the LTE antenna.

6. To protect the connectors from water and dust intrusion, cover all unused connectors with their respective protective caps.



7. One of the following two methods can be chosen to link your PC with the router.

A. Wireless Connection

(a) For Windows user—To link your PC to the router via WiFi, in Microsoft Windows, go to **Control Panel** > **Network Connections**. Right click on **Wireless Network Connection** and choose **View Available Wireless Networks**. Select default SSID [**BR_LTE_xxxx**] and enter default password. Click **Connect**.

(b) For Mac user—Click the on the upper side of the screen to view available wireless networks. Select default SSID [**BR_LTE_xxxx**] and enter default password. Click **Join**.

[Note] The “xxxx” in the example above corresponds to the last 4 digits of MAC address. The default password can be found on the SSID/WPA sticker.

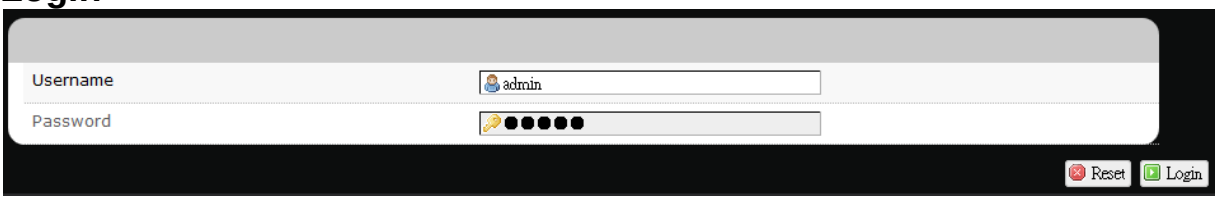
B. Wired Connection

To connect your PC to the router via an Ethernet cable, connect one end of the cable to one of the four LAN ports on the router, and another end of the cable to an Ethernet port on your computer.

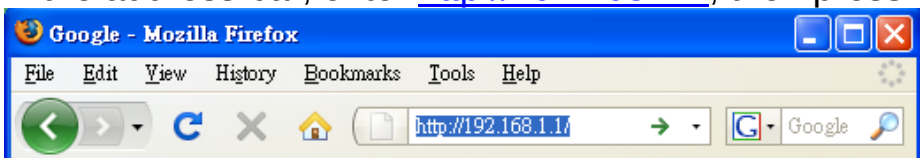
Using Web-based Management

This chapter will guide you on how to configure your router via the web-based utility.

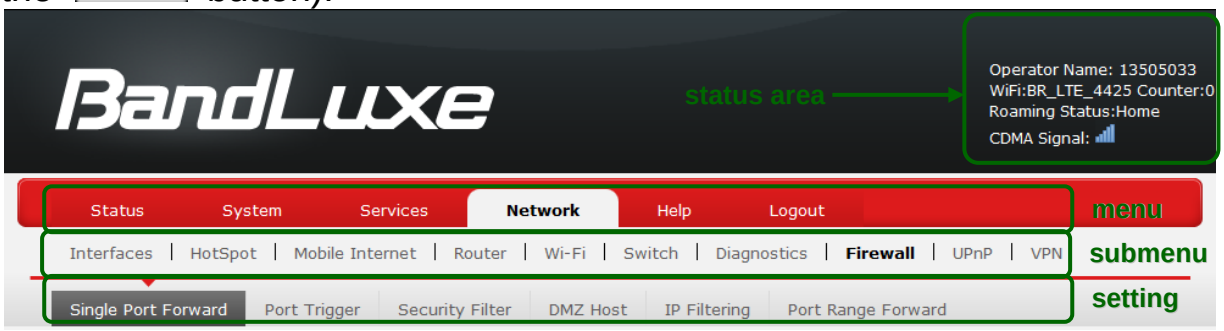
Login



1. Launch a web browser (e.g Mozilla Firefox).
2. In the address bar, enter http://192.168.1.1, then press **Enter**.



3. On the opening screen, enter the username (**admin**) and password (**admin**).
4. Click **Login** to login to the main screen.
5. Click one of the *menu*, *submenu*, and/or *setting* tabs to configure the system. Additionally, the *status area* displays current wireless network information and setting-related messages (e.g. the message **Unapplied Change** appears whenever new settings are temporarily stored in the router without being applied, which will remind you to click the Apply button).

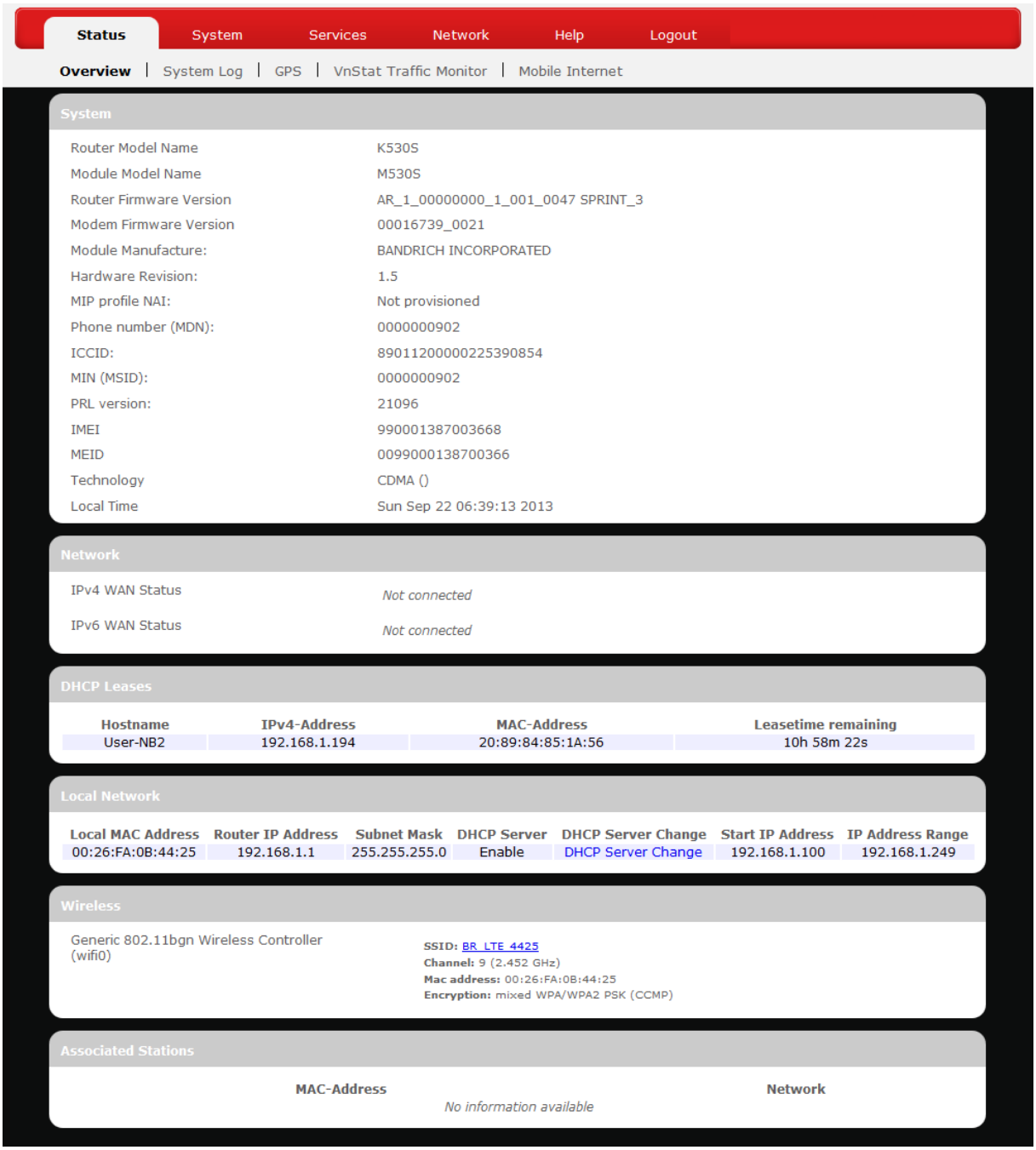

BandLuxe
status area
Operator Name: 13505033
WiFi:BR_LTE_4425 Counter:0
Roaming Status:Home
CDMA Signal:
Status System Services Network Help Logout
menu
Interfaces | HotSpot | Mobile Internet | Router | Wi-Fi | Switch | Diagnostics | Firewall | UPnP | VPN
submenu
Single Port Forward Port Trigger Security Filter DMZ Host IP Filtering Port Range Forward
setting

Note: If SIM Card's PIN verification is needed, select **Network > Mobile Internet > U/SIM PIN Management**.
Enter the PIN code into text box of "**PIN Code Verification**". Click **Verify**.
Mobile internet access will be enabled shortly after.

Status

This menu displays various statuses of the router. The associated submenu items are: **Overview**, **System Log**, **GPS**, **VnStat Traffic Monitor**, and **Mobile Internet**.

Overview



The **Overview** submenu renders complete statistics for the router.

System

Displays system information: router model name, router model name, router firmware version, modem firmware version, mophone number (MDN), ICCID, MIN (MSID), PRL version, IMEI, MEID, and local time.

Network

Displays current network connection information of IPv4 WAN and/or IPv6 WAN: type of network assignment (e.g. DHCP), network address, netmask, gateway, DNS addresses 1 & 2, and time connected since the establishment of the current mobile internet connection.

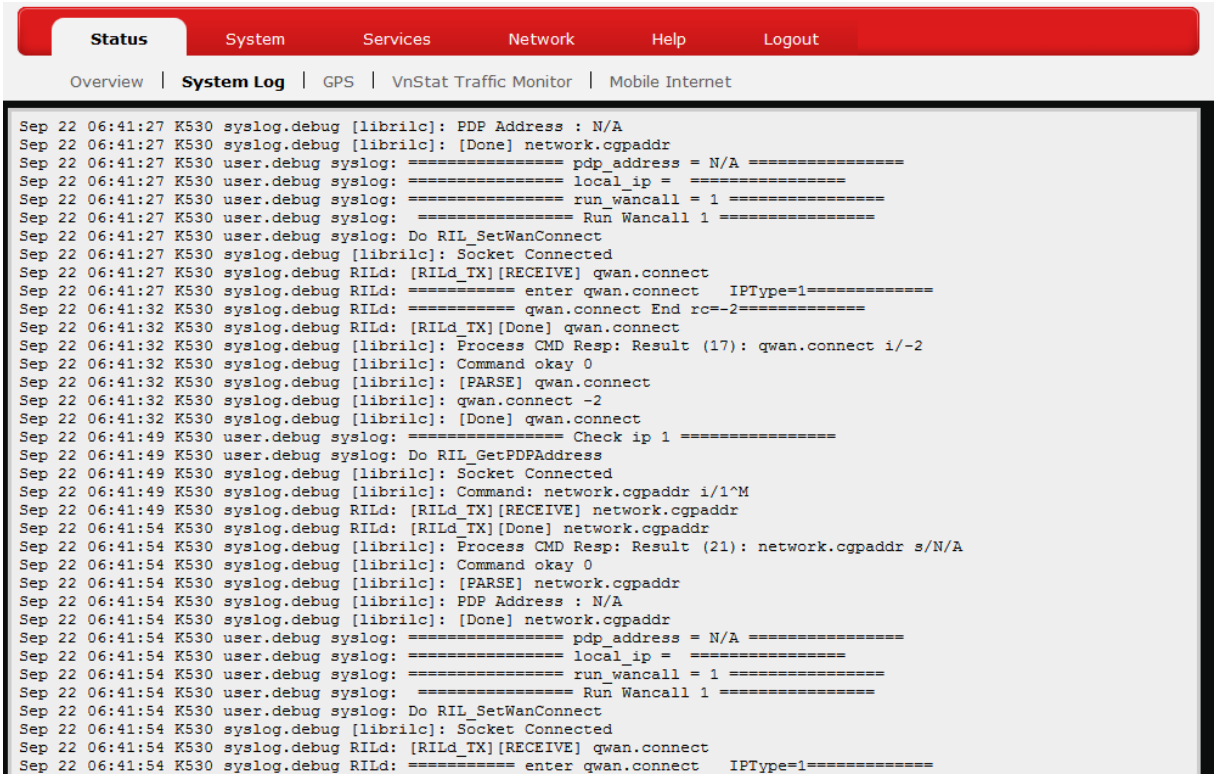
DHCP Leases

Display DHCP lease information for each client: hostname, IPv4 address, MAC address, and lease time remaining.

Local Network

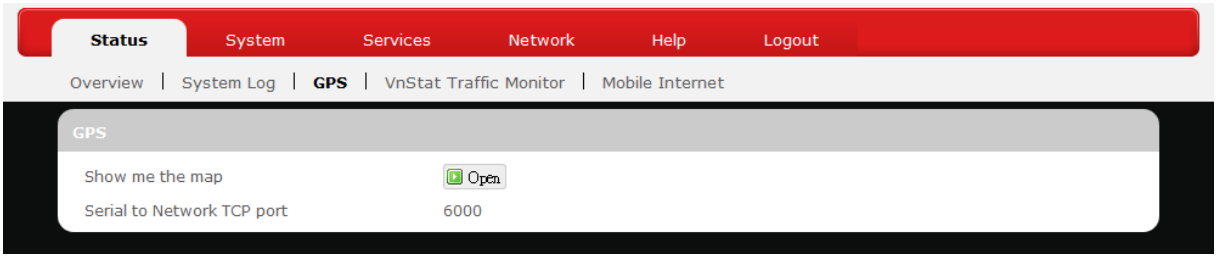
Displays local network information: local MAC address, router IP address, subnet mask, DHCP server, DHCP server change, start IP address, IP and address range

System Log


Status
System
Services
Network
Help
Logout
Overview | System Log | GPS | VnStat Traffic Monitor | Mobile Internet
Sep 22 06:41:27 K530 syslog.debug [librilc]: PDP Address : N/A
Sep 22 06:41:27 K530 syslog.debug [librilc]: [Done] network.cgpaddr
Sep 22 06:41:27 K530 user.debug syslog: ================ pdp_address = N/A ================
Sep 22 06:41:27 K530 user.debug syslog: ================ local_ip = ================
Sep 22 06:41:27 K530 user.debug syslog: ================ run_wancall = 1 ================
Sep 22 06:41:27 K530 user.debug syslog: ================ Run Wancall 1 ================
Sep 22 06:41:27 K530 user.debug syslog: Do RIL_SetWanConnect
Sep 22 06:41:27 K530 syslog.debug [librilc]: Socket Connected
Sep 22 06:41:27 K530 syslog.debug RILd: [RILd_TX][RECEIVE] qwan.connect
Sep 22 06:41:27 K530 syslog.debug RILd: ========== enter qwan.connect IPType=1==========
Sep 22 06:41:32 K530 syslog.debug RILd: ========== qwan.connect End rc=-2==========
Sep 22 06:41:32 K530 syslog.debug RILd: [RILd_TX][Done] qwan.connect
Sep 22 06:41:32 K530 syslog.debug [librilc]: Process CMD Resp: Result (17): qwan.connect i/-2
Sep 22 06:41:32 K530 syslog.debug [librilc]: Command okay 0
Sep 22 06:41:32 K530 syslog.debug [librilc]: [PARSE] qwan.connect
Sep 22 06:41:32 K530 syslog.debug [librilc]: qwan.connect -2
Sep 22 06:41:32 K530 syslog.debug [librilc]: [Done] qwan.connect
Sep 22 06:41:49 K530 user.debug syslog: ================ Check ip 1 ================
Sep 22 06:41:49 K530 user.debug syslog: Do RIL_GetPDPAddress
Sep 22 06:41:49 K530 syslog.debug [librilc]: Socket Connected
Sep 22 06:41:49 K530 syslog.debug [librilc]: Command: network.cgpaddr i/1^M
Sep 22 06:41:49 K530 syslog.debug RILd: [RILd_TX][RECEIVE] network.cgpaddr
Sep 22 06:41:54 K530 syslog.debug RILd: [RILd_TX][Done] network.cgpaddr
Sep 22 06:41:54 K530 syslog.debug [librilc]: Process CMD Resp: Result (21): network.cgpaddr s/N/A
Sep 22 06:41:54 K530 syslog.debug [librilc]: Command okay 0
Sep 22 06:41:54 K530 syslog.debug [librilc]: [PARSE] network.cgpaddr
Sep 22 06:41:54 K530 syslog.debug [librilc]: PDP Address : N/A
Sep 22 06:41:54 K530 syslog.debug [librilc]: [Done] network.cgpaddr
Sep 22 06:41:54 K530 user.debug syslog: ================ pdp_address = N/A ================
Sep 22 06:41:54 K530 user.debug syslog: ================ local_ip = ================
Sep 22 06:41:54 K530 user.debug syslog: ================ run_wancall = 1 ================
Sep 22 06:41:54 K530 user.debug syslog: ================ Run Wancall 1 ================
Sep 22 06:41:54 K530 user.debug syslog: Do RIL_SetWanConnect
Sep 22 06:41:54 K530 syslog.debug [librilc]: Socket Connected
Sep 22 06:41:54 K530 syslog.debug RILd: [RILd_TX][RECEIVE] qwan.connect
Sep 22 06:41:54 K530 syslog.debug RILd: ========== enter qwan.connect IPType=1==========

The **System Log** submenu tracks system activities after power on.

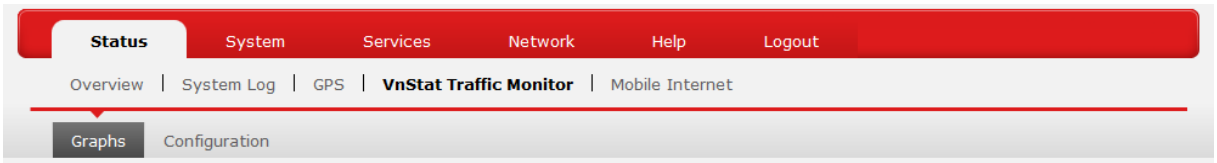
GPS



The **GPS** submenu displays Global Positioning System information. Click

to proceed.

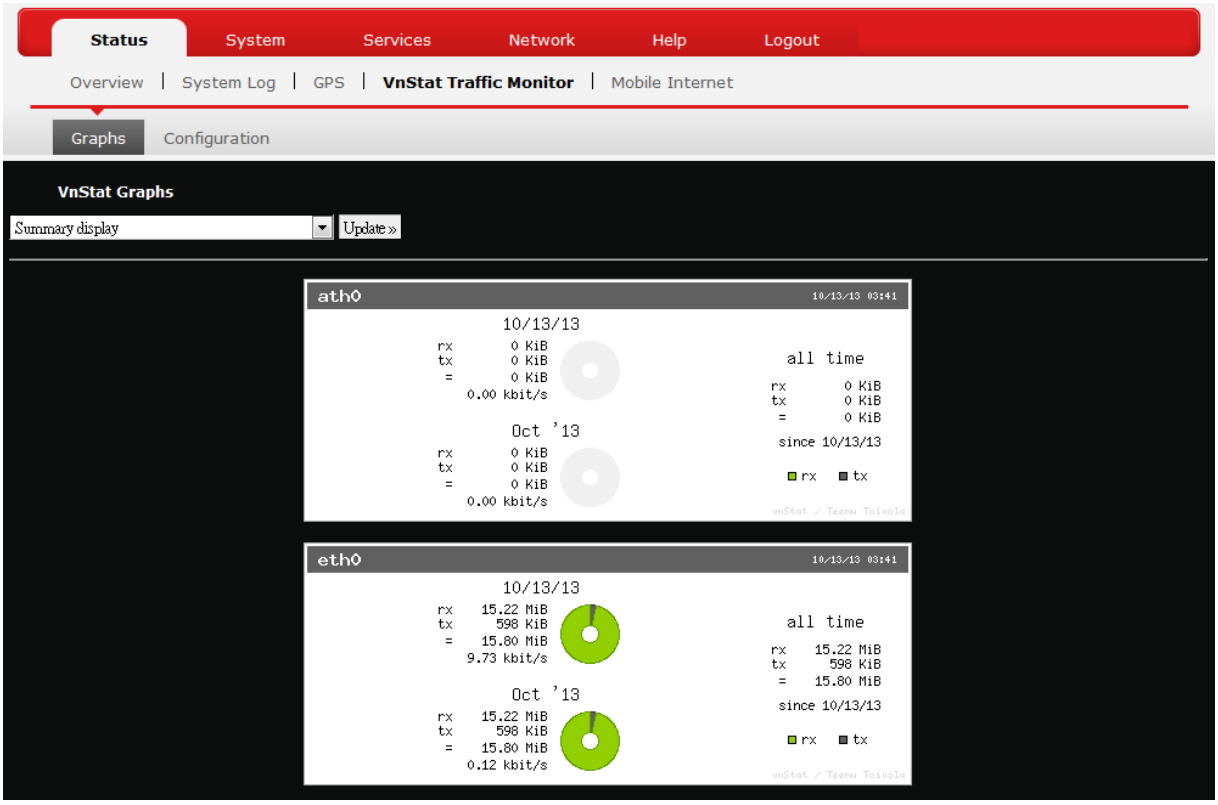
VnStat Traffic Monitor



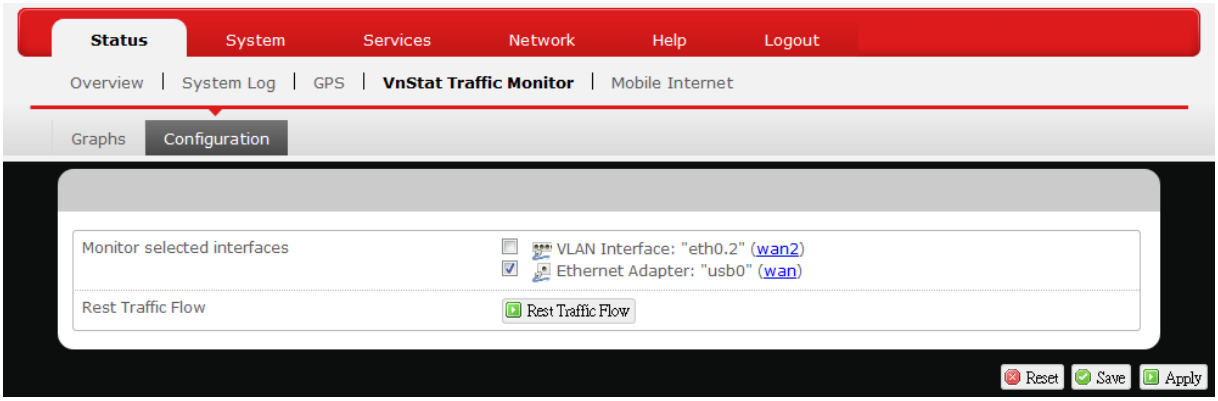
The **VnStat Traffic Monitor** submenu displays graphic analysis of the router's network traffic history.

Graphs

Displays VnStat network traffic history in various graphic analysis options: **Summary display**, **Top 10 display**, **Hourly traffic**, **Daily traffic**, and **Monthly traffic**. Click ▼, select an analysis option from the drop-down list, and click **Update**. The VnStat Graphs will be updated accordingly.



Configuration

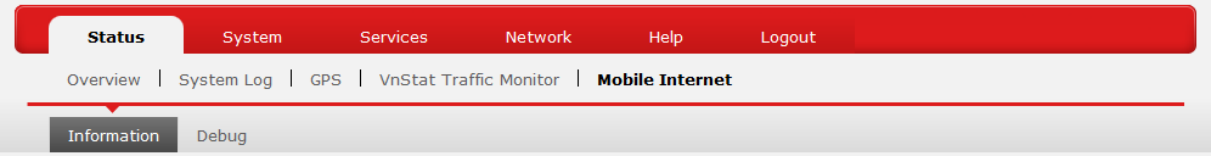


VnStat Traffic Monitor configurations can be made here.

a) *Monitor selected devices:* Click the checkbox to enable/disable network monitoring of the displayed interface(s). Click the link wan or wan2 to jump to the associated **Common Configuration** setting under the submenu **Network ➔ Interfaces**.

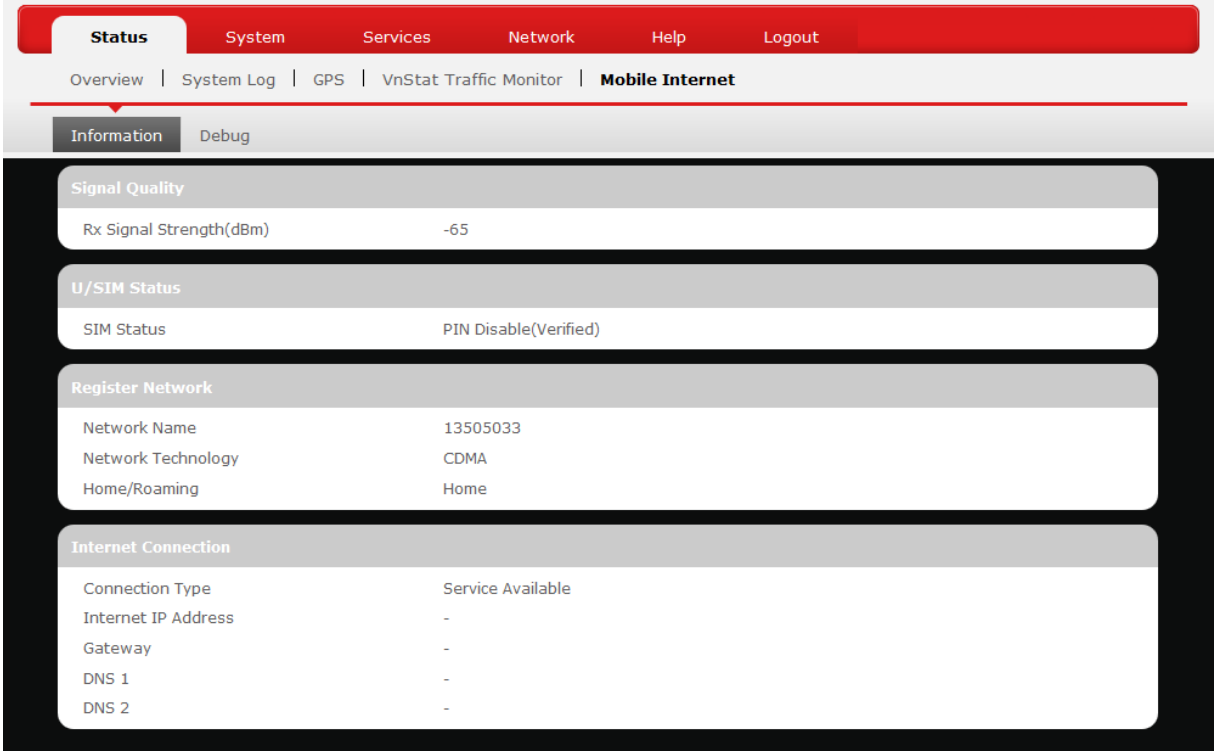
b) *Rest Traffic Flow:* Click to discard previous network history log and start anew.

Mobile Internet



The **Mobile Internet** submenu displays mobile internet statistics along with a debug tool. It has two submenu settings: **Information** and **Debug**.

Information



Signal Quality

Displays signal strength of current mobile internet connection in dBm.

U/SIM Status

Displays current SIM card status:

a) *Read SIM Fail* – No valid SIM card is inserted

b) *PIN Disable(Verified)* – PIN protection is disabled while the SIM card

status is verified; mobile internet service is available with this status.

c) *PIN Enable(No Verified/Retries:#)* – PIN protection is enabled while the SIM card verification is pending (whereas # is the number of allowed PIN verifications remaining before SIM lock occurs).

d) *PIN Enable(Verified)* – PIN protection is enabled while the SIM card status is verified; mobile internet service is available with this status.

Registered Network

a) *Network Name* – Name of your mobile internet service provider

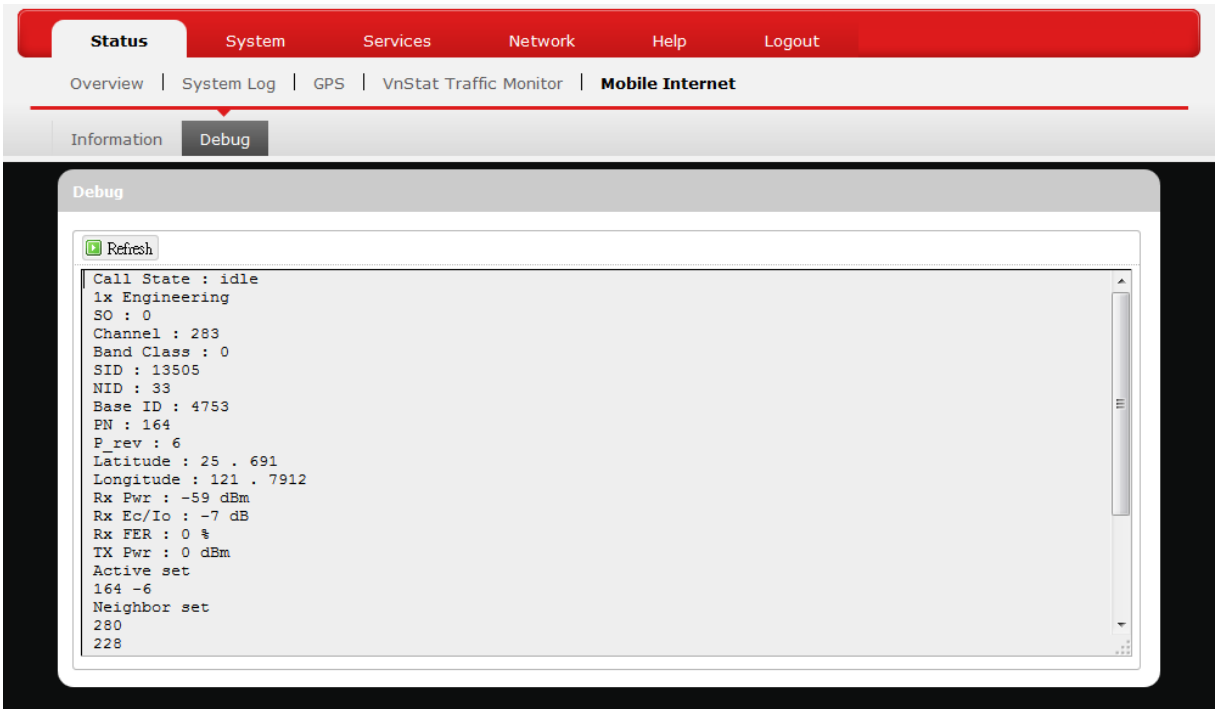
b) *Network Technology* – Mobile internet communication signal type. Examples are WCDMA (3G) and LTE (4G).

c) *Home/Roaming* – Displays current network roaming status:
Home indicates mobile internet connection to the home location where the SIM card service is registered. Roaming indicates the extended mobile internet connection service in a location different from the home location where the SIM card service is registered. An example of roaming is when you travel abroad.

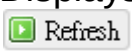
Internet Connection

Displays information of current internet connection:
Connection Type, Internet IP Address, Gateway, and DNS 1/2.

Debug



Debug

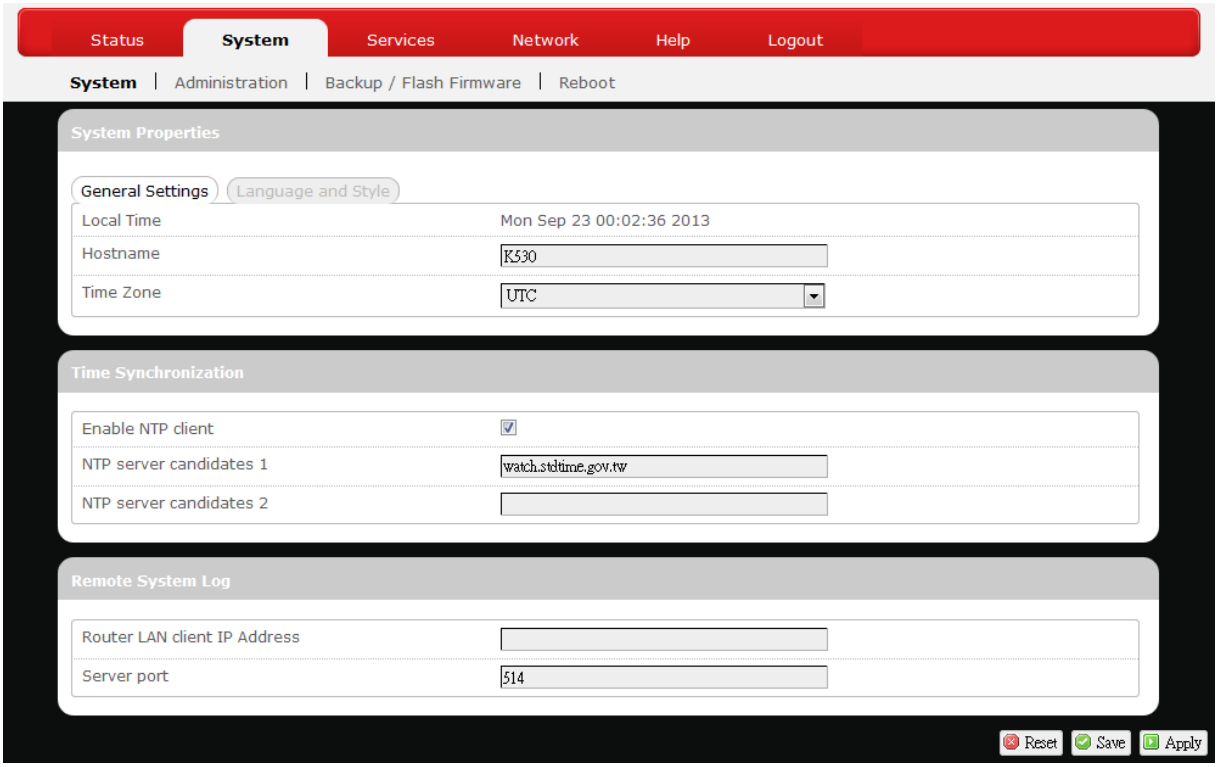
Displays mobile internet statistics for analysis and troubleshooting. Click 

to update the statistics.

System

This menu is for system information and configurations.

System



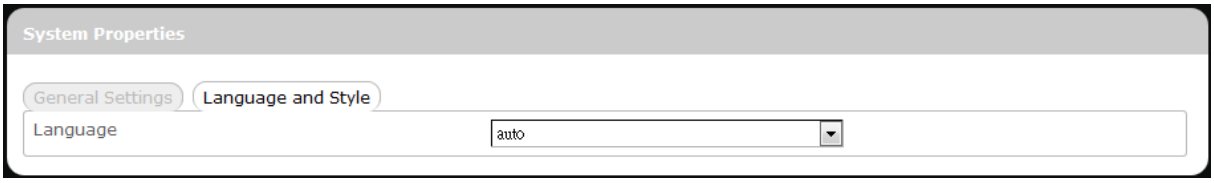
System Properties

Click either the “General Settings” or “Language and Style” tab to configure their respective settings.

General Settings

Local Time – Displays current local time. To synchronize local time with the browser, click Sync with browser.
Hostname – Enter the desired hostname in this check field.
Time Zone – Sets the time zone associated with this router. Click on and select the desired region.

Language and Style



Language – Sets the desired display language and style of the router. Click ▼ and select the desired display language and style.

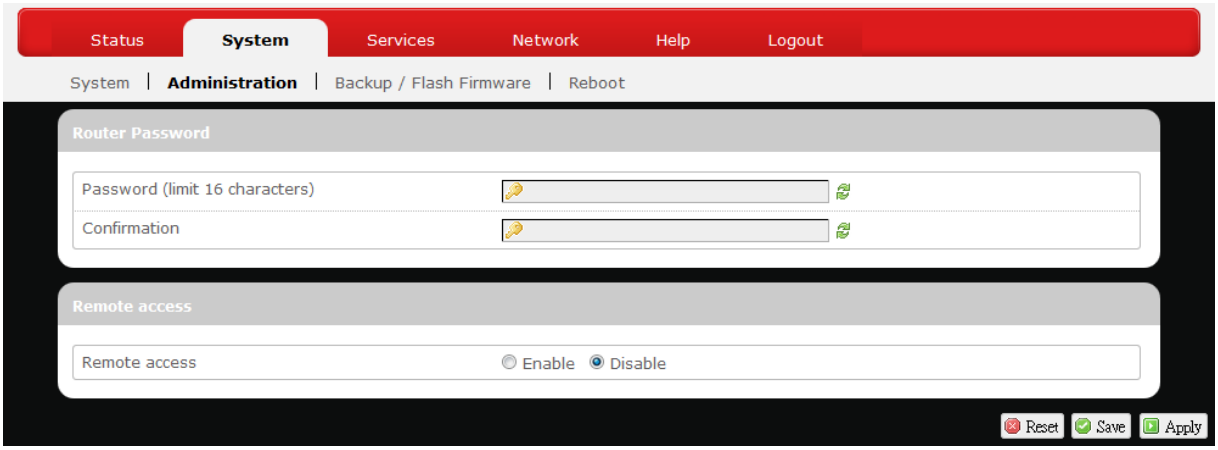
Time Synchronization

Enable NTP client: Click the checkbox to enable/disable. With this option enabled, two more options will appear– “Provide NTP server” and “NTP server candidates”.
NTP server candidates 1/2: Enter the desired server candidates here.

Remote System Log

Router LAN client IP address: Displays the client IP address of the router LAN.
Server port: Displays port number of the server.

Administration

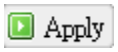


Router Password

Login password of the router can be changed here. Enter the new password in the ‘Password’ field, and enter the same password once again in the ‘Confirmation’ field.

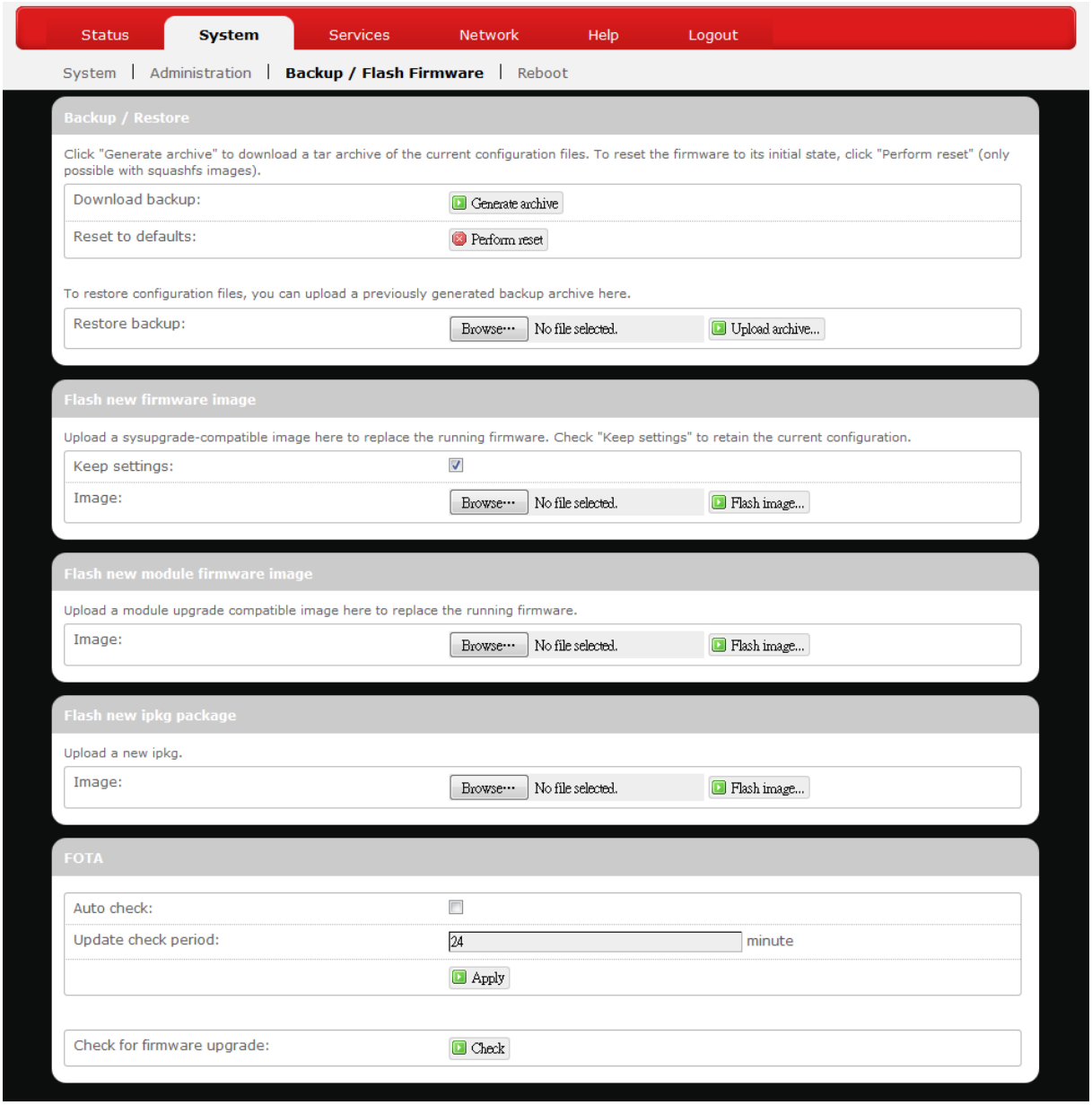
Remote Access

This field specifies whether or not to allow remote access of this router.

After changing password and/or specifying remote access, click 

. The screen will display a confirmation message after successful password change.

Backup / Flash Firmware



Backup / Restore

Download backup

Here you can backup all current settings of the router to a TAR archive file on your computer or mobile device. Just click

. A dialog window will prompt you to open or save the archive file. Depending on the browser that you are using, the TAR file may be saved in the system download folder or a location of your choice.

Reset to defaults

Here you can restore the router to its original factory settings. Just click Perform reset, and a dialog message will appear to indicate the factory reset process. After completion of the reset process, the router will automatically reboot and return to its initial login prompt.

Restore backup

Here you can restore router settings previously saved as a TAR archive file on your computer or mobile device. Just click Browse... to find and select the previously saved TAR archive file, and then click 'Open'. Confirm that the TAR filename appears beside the Browse... button and click Upload archive... . The system will reboot after completion of backup restoration.

Flash new firmware image

This option allows you to upgrade this router with the updated firmware image. Just click Browse... to find and select the firmware image file, and then click 'Open'. Confirm that the firmware filename appears beside the Browse... button and click Flash image... . The system will reboot after successful upgrade.

Flash new module firmware image

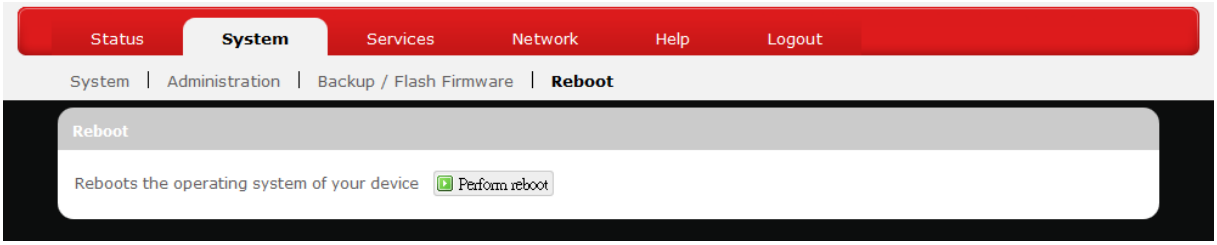
This option allows you to upgrade this router with the updated module firmware image. Just click Browse... to find and select the firmware package file, and then click 'Open'. Confirm that the firmware filename appears beside the Browse... button and click Flash image... . The system will reboot after successful upgrade.

Flash new ipkg package

This option allows you to upgrade this router with the updated IPKG package. Just click Browse... to find and select the IPKG package file, and then click 'Open'. Confirm that the IPKG package filename appears beside the Browse... button and click Flash image... .

Warning: Upgrading firmware may take a few minutes; do not turn off the power or press the Reset button during upgrade.

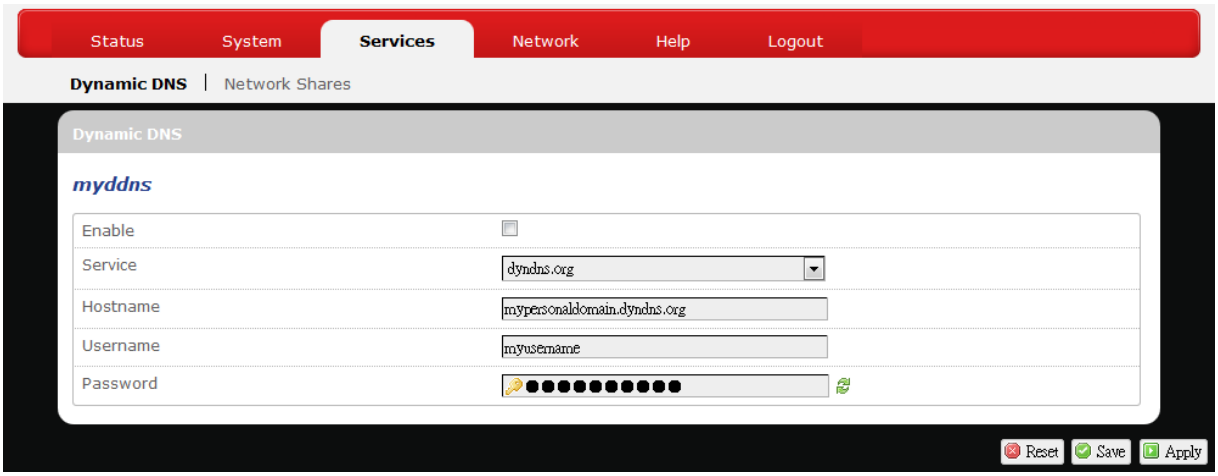
Reboot



Click ‘Perform reboot’ to restart the router.

Services

Dynamic DNS



The **Services** menu hosts configuration options for **Dynamic Domain Name Service (DDNS)**, which is a system that allows the domain name data held in a name server to be updated in real time. It allows an Internet domain name to be assigned to a computer with a varying (dynamic) IP address. Before you can use this feature, you need to sign up for DDNS with a DDNS provider, www.dyndns.org or www.TZO.com.

Enable: Check or un-check this box to enable or disable DDNS.

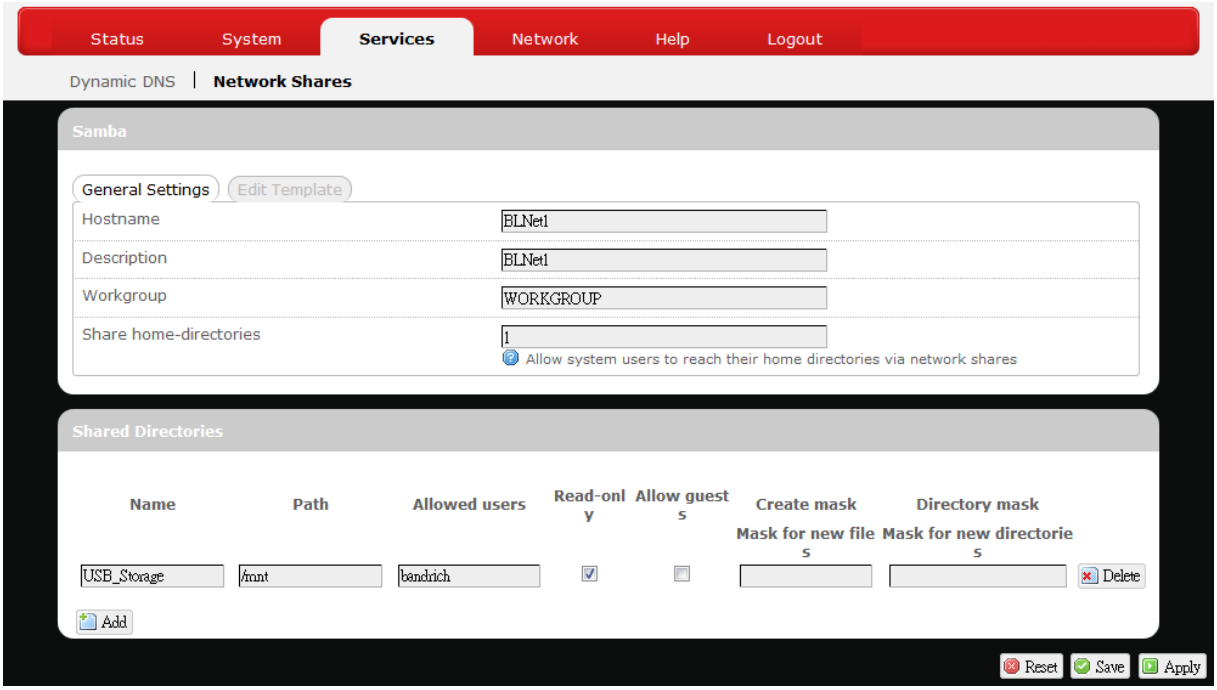
Service: Specifies the DDNS service URL. From the drop-down list, click and select an URL from the list.

Hostname: Enter the hostname for your DDNS account.

Username: Enter the username for your DDNS account.

Password: Enter the password for your DDNS account.

Network Shares



The **Network Shares** submenu hosts configuration options for sharing the USB storage drive on the network.

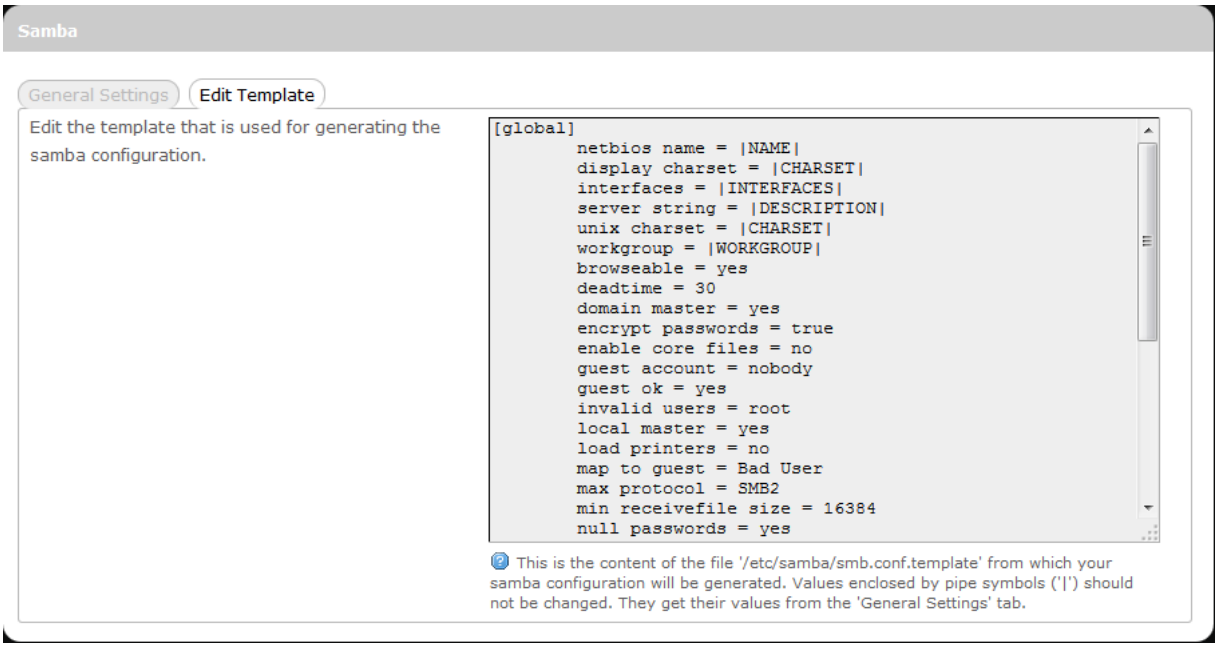
Samba

This section is for detailed configurations of Samba server, which sets up this router as the USB storage drive server.

General Settings

Hostname:	Specify host name to be seen on the network.
Description:	Specify description for the host.
Workgroup:	Specify workgroup name (e.g. WORKGROUP).
Share home-directories:	This option allows system users to reach their home directories via network sharing..

Edit template


Samba
General Settings
Edit Template
Edit the template that is used for generating the samba configuration.
[global]
netbios name = |NAME|
display charset = |CHARSET|
interfaces = |INTERFACES|
server string = |DESCRIPTION|
unix charset = |CHARSET|
workgroup = |WORKGROUP|
browseable = yes
deadtime = 30
domain master = yes
encrypt passwords = true
enable core files = no
guest account = nobody
guest ok = yes
invalid users = root
local master = yes
load printers = no
map to guest = Bad User
max protocol = SMB2
min receivefile size = 16384
null passwords = yes
This is the content of the file '/etc/samba/smb.conf.template' from which your samba configuration will be generated. Values enclosed by pipe symbols ('|') should not be changed. They get their values from the 'General Settings' tab.

This section is for advanced users to edit the template used for generating Samba configuration.

Shared Directories

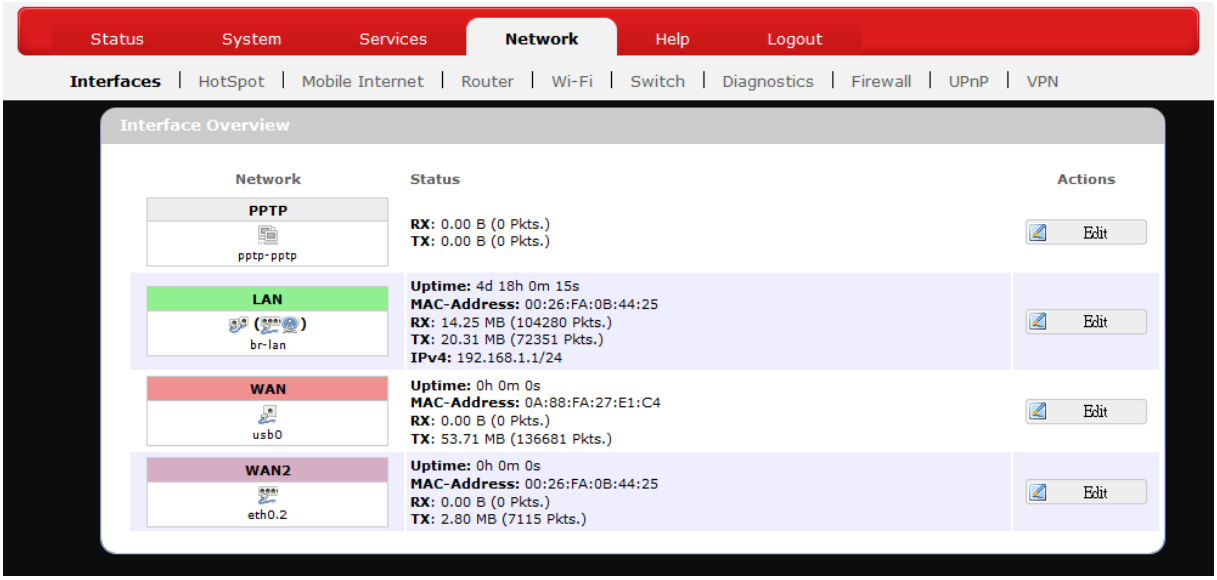
This section is for detailed configurations of shared directories. To add a directory for sharing, click Add. To remove a directory for sharing, click the corresponding Delete button. In the status area, the message **Unapplied Change** may appear next to “Operator Name” to indicate configuration changes temporarily stored in the router.

Name:	Specifies name of the shared directory.
Path:	Specifies the complete path of the directory.
Allowed users:	Specifies the samba users that will be allowed to access the shared directories.
Read only:	Enables or disables the read-only option for the shared directory.
Allow guests:	Enables or disables guest access for the shared directory.
Create mask (Mask for new files):	Changes file access permissions according to the integer code entered. This field is equivalent to the *chmod* command of the Linux/Unix operating systems.
Directory mask	Changes directory access permissions according to

(Mask for new directories): the integer code entered. This field is equivalent to the *chmod* command of the Linux/Unix operating systems.

Network

Interfaces



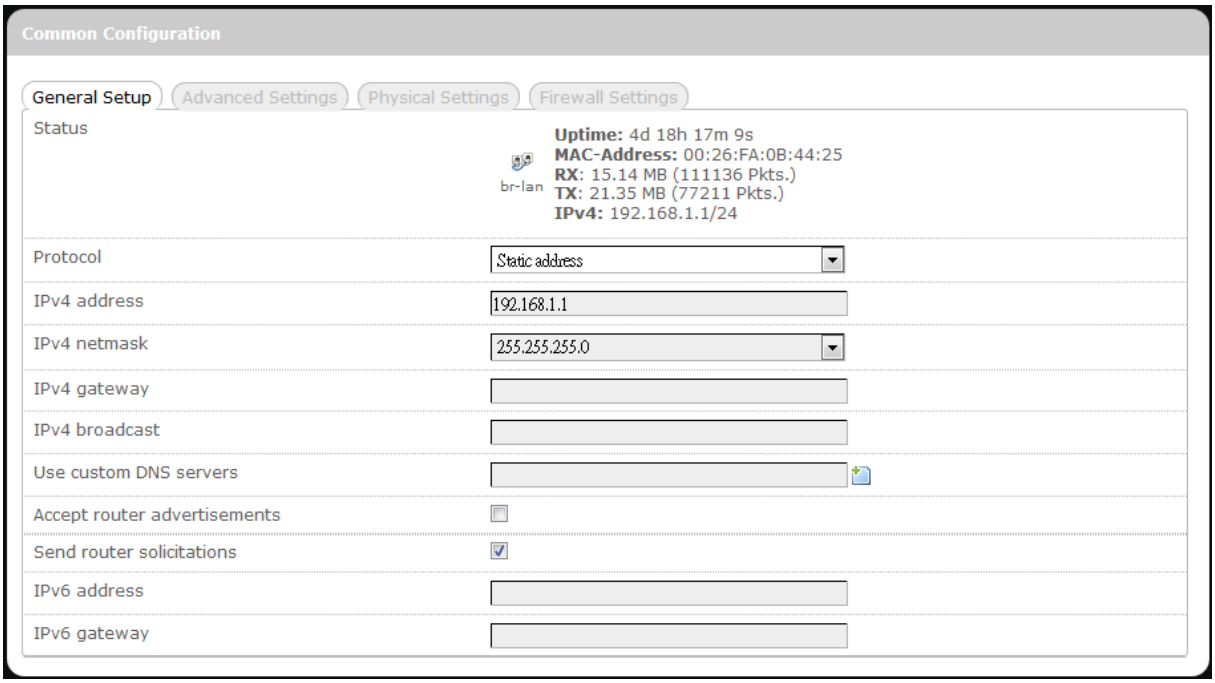
The **Interfaces** submenu allows interface configurations of different networks connected to this router. The configuration items are the same for each network with different default settings.

Interface Overview

Here you can see the brief network status summary for PPTP (Point-to-Point Tunneling Protocol), LAN (local area network), WAN (wide area network), and WAN2 (wide area network 2). To configure LAN or WAN interfaces, click the appropriate **Edit** button and follow the below section *Common Configuration* for more details.

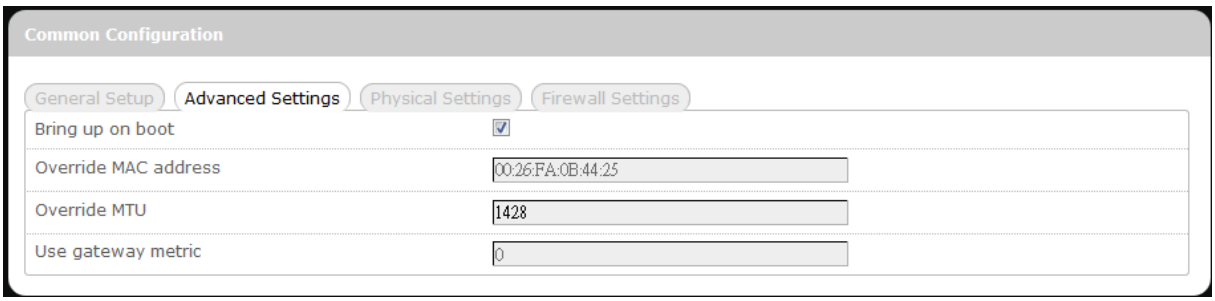
Common Configuration

General Setup



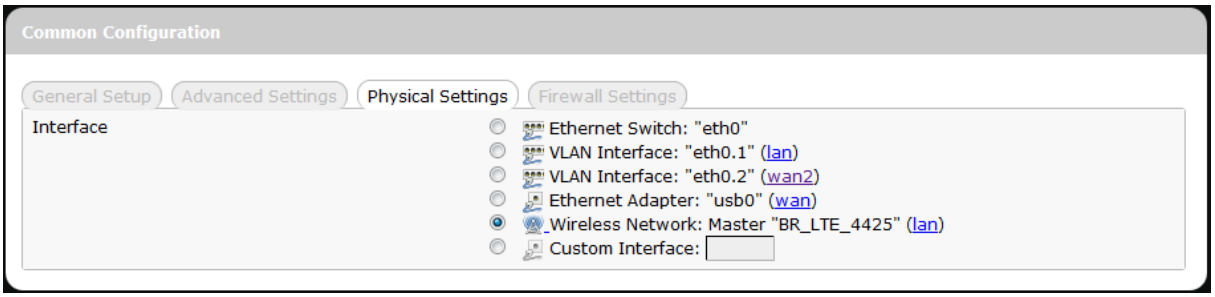
Status:	Displays protocol-dependent statistics of network connection.
Protocol:	Specifies the protocol to be used for the network. The available protocols are *Static address*, *DHCP client*, *Unmanaged*, *PPP*, *PPtP*, *PPPoE*, *PPPoATM*, *UTMS/GPRS/EV-DO*, and *L2TP*.
Really switch protocol:	This configuration item appears when the protocol is changed. Press Switch protocol to confirm protocol change and show protocol-dependent configuration items.
(Protocol-dependent configuration items):	Different protocol-dependent configuration items will appear according to the protocol chosen.

Advanced Settings



This tab is for advanced users to make detailed configurations of protocol-related settings. Actual configuration items will vary according to the protocol chosen in the tab item *General Setup*.

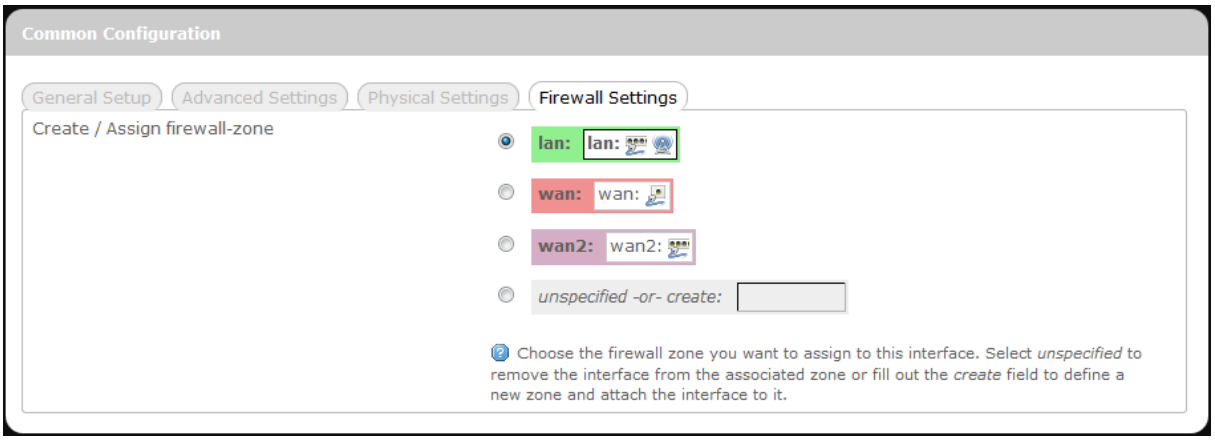
Physical Settings



This tab is for selection of physical interface of the associated network. Click one of the available physical interfaces or click Custom Interface: and enter your own interface name.

This tab is not available for the following protocols: *PPP*, *PPtP*, *PPPoE*, *PPPoATM*, *UTMS/GPRS/EV-DO*, and *L2TP*.

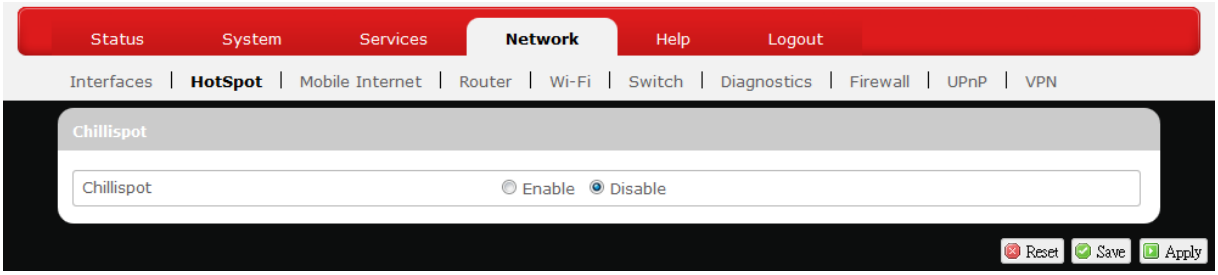
Firewall Settings


Common Configuration
General Setup
Advanced Settings
Physical Settings
Firewall Settings
Create / Assign firewall-zone
lan: lan:
wan: wan:
wan2: wan2:
unspecified -or- create:
Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

This tab is for adjustment of firewall settings.

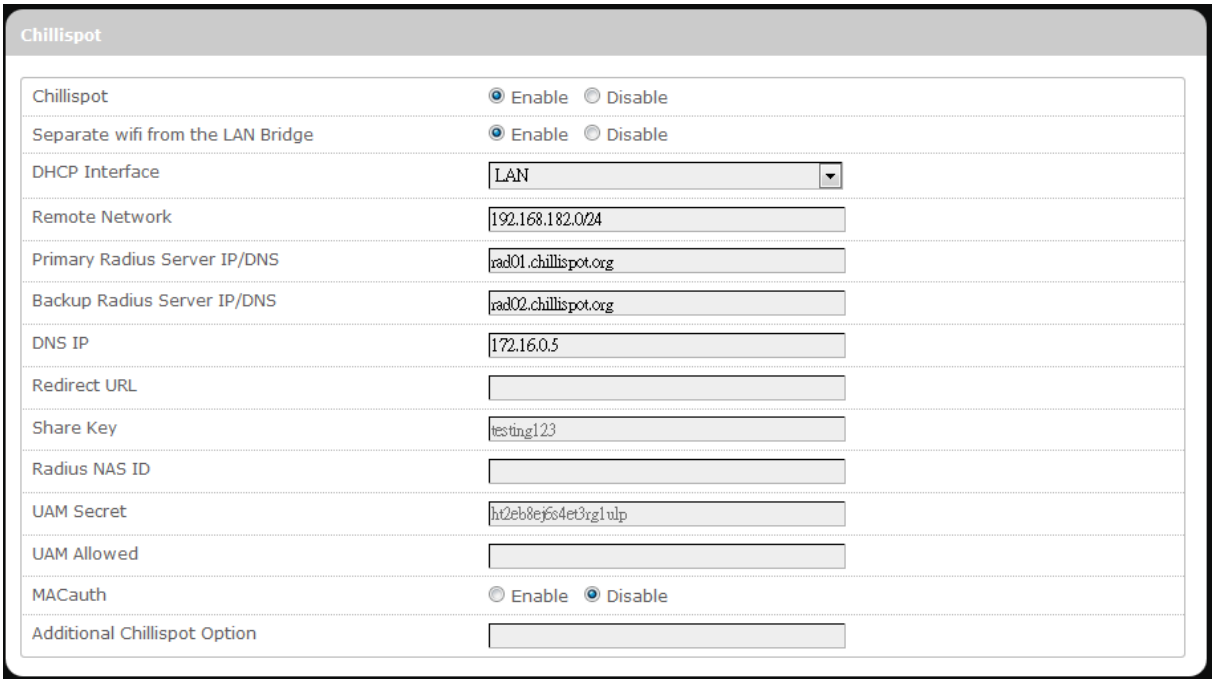
Click the desired network as the desired firewall zone assigned to this interface. Furthermore, you can remove the interface from the associated zone by entering “unspecified” in the *unspecified -or- create* field and clicking Apply, or you can define a new zone by entering your own firewall name in the *unspecified -or- create* field and clicking Apply.

Hotspot



The **Hotspot** submenu is for setup and adjustment of mobile internet connection through WLAN (wireless local area network).

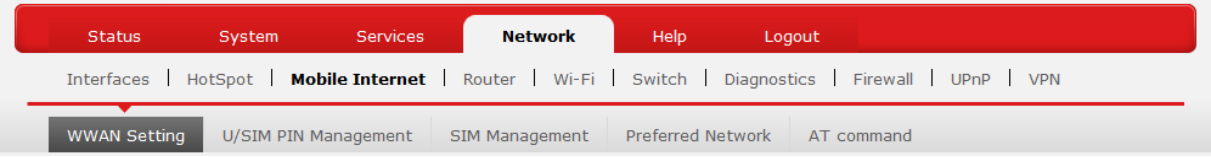
Chillispot



Chillispot:	Enable or disable the chillispot (i.e. hotspot) feature.
Separate WiFi from the LAN Bridge:	Enable or disable WiFi separation from the LAN bridge. If this option is enabled, two additional configuration items, *DHCP Interface* and *Remote Network*, will appear below.
DHCP Interface:	Select the appropriate DHCP interface when the configuration item "*WiFi separation from the LAN bridge*" is enabled. The options are *LAN*, *WAN*, or *WLAN&LAN*.
Remote Network:	Enter the IP address of remote network when the configuration item "*WiFi separation from the LAN*

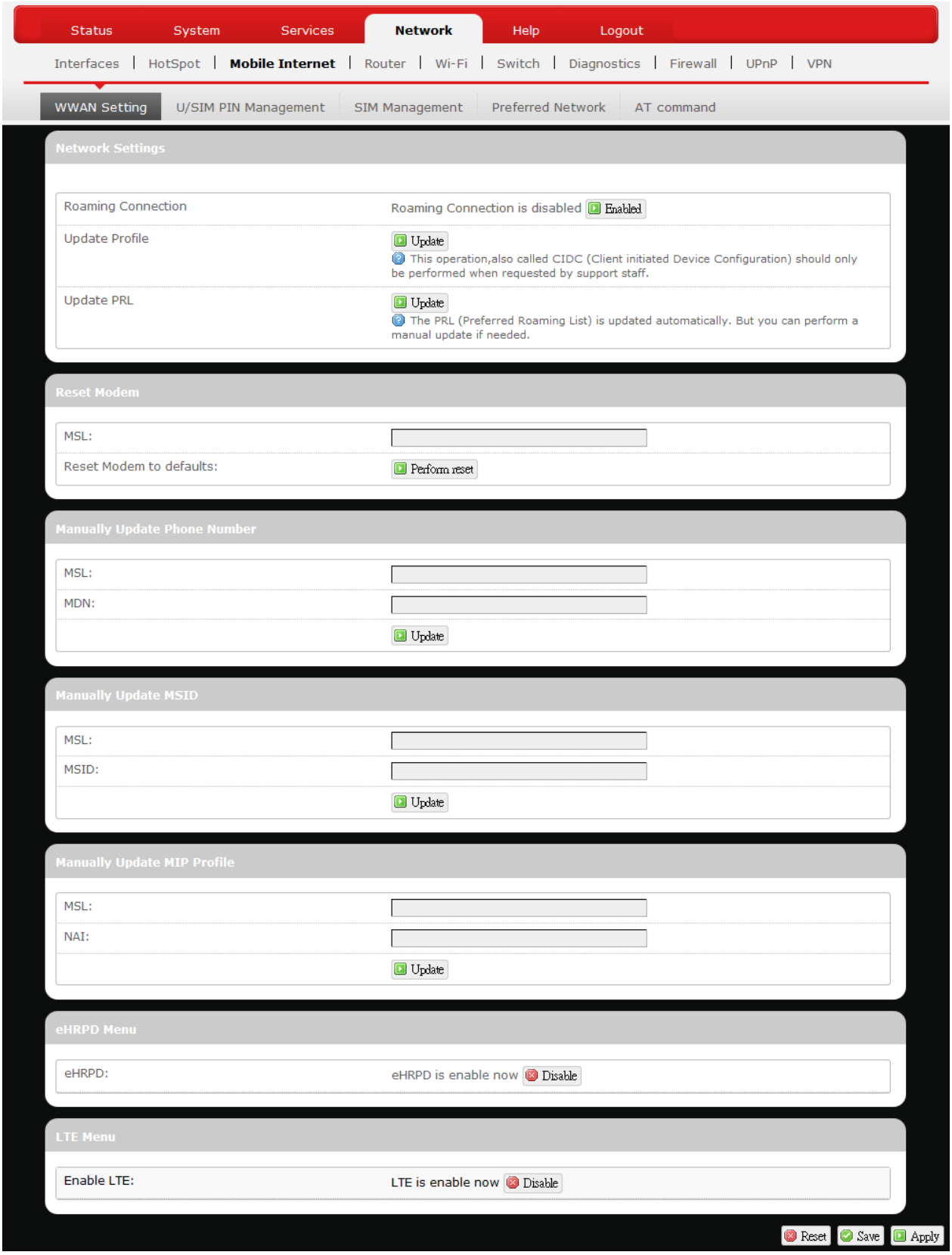
	bridge" is enabled.
Primary RADIUS Server IP/DNS:	Enter the IP/DNS address of primary RADIUS server.
Backup RADIUS Server IP/DNS:	Enter the IP/DNS address of backup RADIUS server.
DNS IP:	Enter the numerical IP address of DNS.
Redirect URL:	Enter the redirection URL if needed.
Share key:	Enter the share key here.
RADIUS NAS ID:	Enter the NAS ID for RADIUS authentication.
UAM Secret:	Enter the secret code for UAM (universal access method).
UAM Allowed:	Enter the name for UAM allowed.
MACauth:	Enable or disables MAC authorization.
Additional Chillispot Option:	Enter the additional chillispot option if needed.

Mobile Internet



The **Mobile Internet** submenu is for setup and adjustment of mobile internet connection and furthermore has four setting tabs: **WWAN Setting**, **U/SIM PIN Management**, **SIM Management**, and **Preferred Network**.

WWAN Setting



Network Settings

Roaming Connection:	Click **Enable** to enable connection in roaming mode.
Update Profile:	Click **Update** to update the network profile.
Update PRL:	Click **Update** to update the PRL (Preferred Roaming List).

Reset Modem

Enter the *MSL* (Maximum Segment Lifetime) when needed.

Click **Perform reset** to reset this modem to its factory default settings.

Manually Update Phone Number

To update the mobile device phone number, , enter the *MSL* and *MDN* (Mobile Directory Number) as needed, then click **Update**.

Manually Update MSID

To update the *MSID* (Mobile Station Identification), enter the *MSL* and *MSID* as needed, then click **Update**.

Manually Update MIP Profile

To update the *MIP* (Mobile Internet Protocol) profile, enter the *MSL* and *NAI* (Network Access Identifier) as needed, then click **Update**.

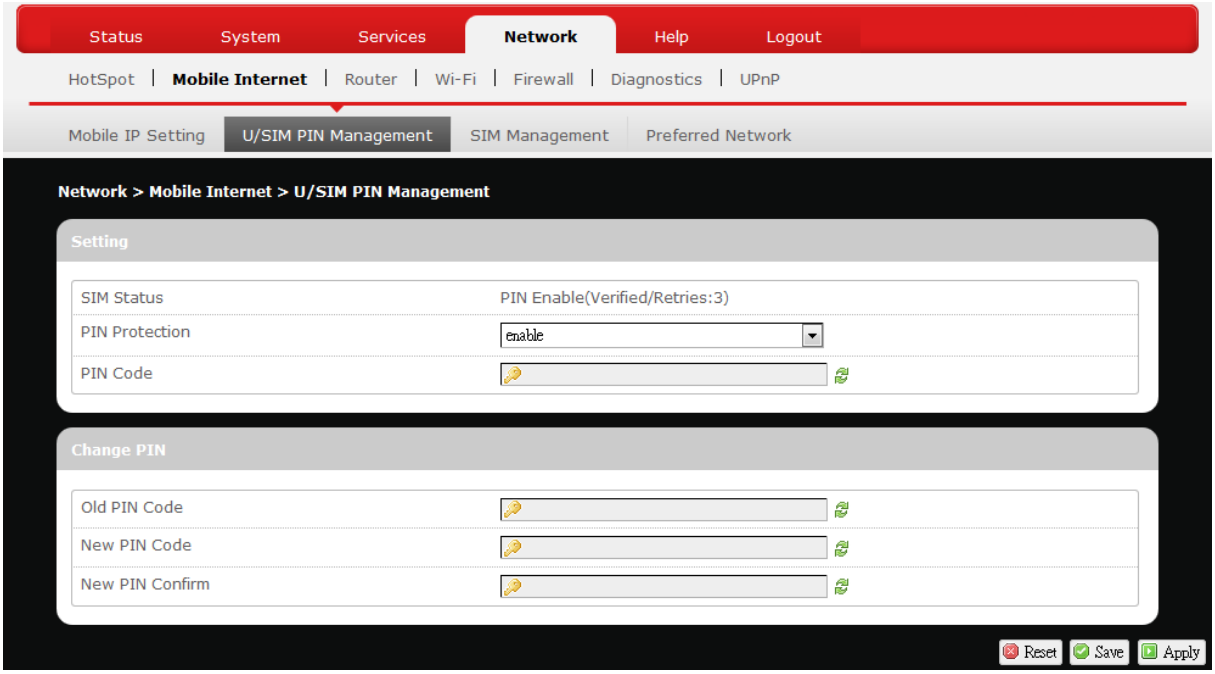
eHRPD Menu

Click the appropriate button to enable or disable eHRPD (Evolved High Rate Packet Data) Menu.

Enable LTE

Click the appropriate button to enable or disable 4G LTE connection.

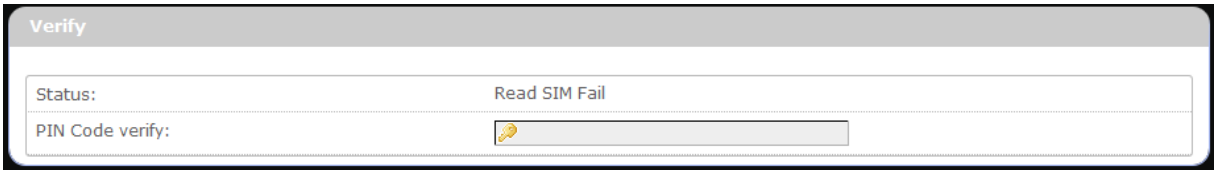
U/SIM PIN Management



This submenu features configurable items that are dependent on the router's mobile internet status, as detailed below.

Scenario 1: No mobile internet service

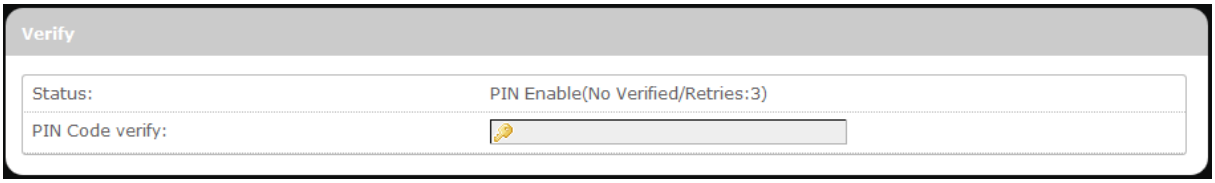
Without a valid SIM card inserted into the router, the Verify dialog will show the following SIM card status:



Here the Verify dialog shows SIM status as "Read SIM Fail", meaning that no valid SIM card is inserted.

Scenario 2: Mobile internet service pending

If a valid SIM card is inserted into the router requiring PIN code verification, the Verify dialog will show the following SIM card status:



Here the Verify dialog shows the SIM status as "No Verified/Retries:3", meaning that a valid SIM card is inserted with PIN code verification pending. Enter your SIM card verification code in the text box of "PIN

Code verify:", and then click

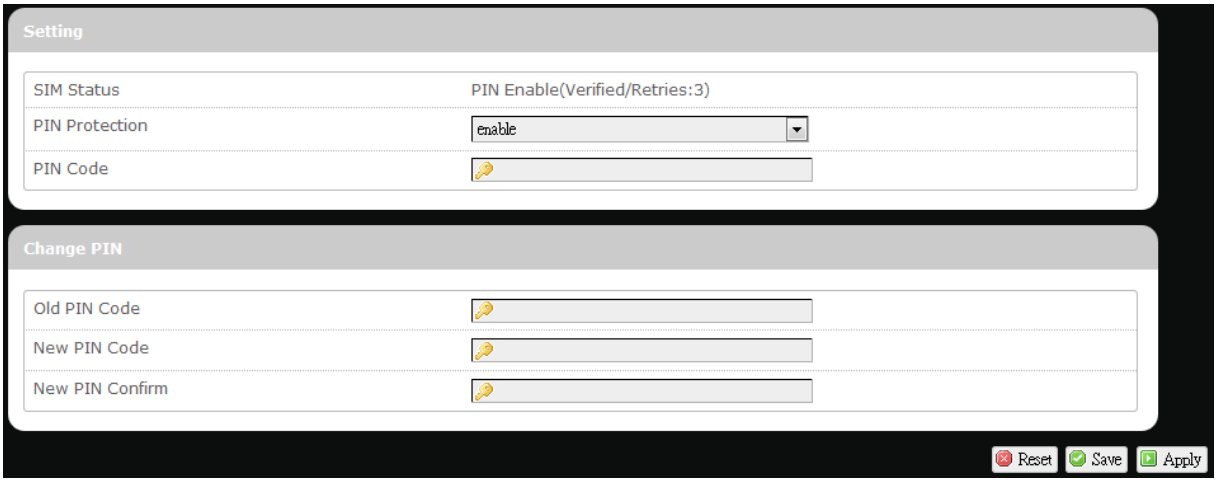
. Once the PIN code verification is finished, the router is ready to use the SIM card's associated mobile internet access, and the top right status area will be updated accordingly.

Operator Name:	Displays the name of the internet service provider
WiFi:	Shows the active WiFi SSID of this router
Counter:	Shows number of clients currently connected to the active SSID
Roaming Status:	Displays current roaming status
(Carrier) Signal:	Displays strength of the indicated signal type (Carrier) For example: 1. Without mobile internet connection, the display will be (no signal). 2. If CDMA (3G) mobile internet connection is established, the display will be (CDMA carrier, excellent signal strength).

Scenario 3: Mobile internet service enabled

If a valid SIM card is inserted into the router with PIN code verified, the configuration dialog will be 'Setting' and/or "Change PIN" to allow further SIM card management (click

after making changes):



Setting

SIM Status: Shows current SIM card status.
"*PIN Enable*" means that the SIM card is enabled for mobile internet access.
"*PIN Disable(Verified/Retries:#)*" means that the SIM card is enabled for mobile internet access without requiring PIN code verification. Note that if PIN protection is re-enabled, # is the number of allowed PIN verifications remaining before SIM lock occurs.

PIN Protection: Enables or disables the PIN protection by clicking and making the appropriate choice from the drop-down list.

PIN Code: If PIN protection is enabled, you need to enter PIN code in this text box for making changes in this 'Setting' dialog.

Change PIN

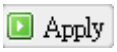
This option is configurable only if PIN Protection is enabled.

Here you can change the PIN code for enhanced SIM card security.

Old PIN Code: Enter the old PIN code.

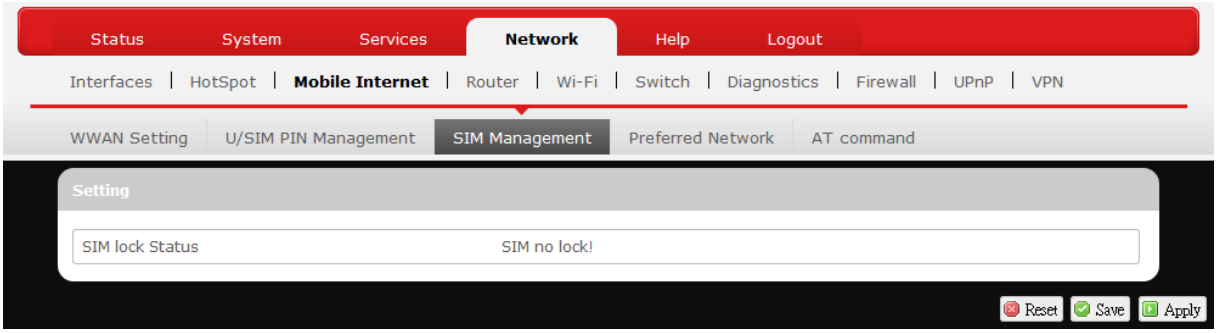
New PIN code: Enter the new PIN code.

New PIN code confirm: Enter the same new PIN code again for PIN code confirmation.

Click 

after making changes in 'Setting' and/or "Change PIN".

SIM Management



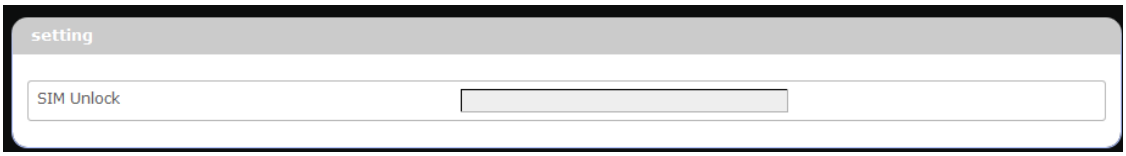
Here you can see the current SIM lock status.

Scenario 1: SIM lock absent

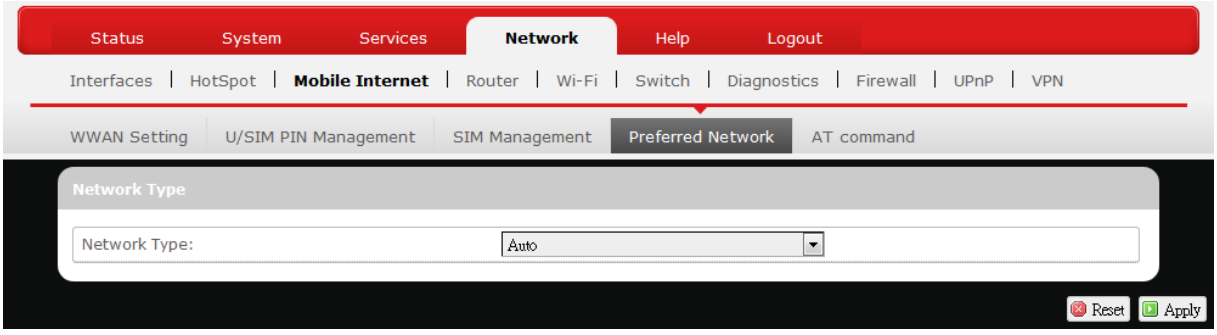
"There is no SIM lock" means the SIM card can be used on this device.

Scenario 2: SIM lock present

If the status shows "Invalid SIM", it means the SIM card is blocked to use on this device. Please contact the operator to get unlock code to unlock, click Apply.

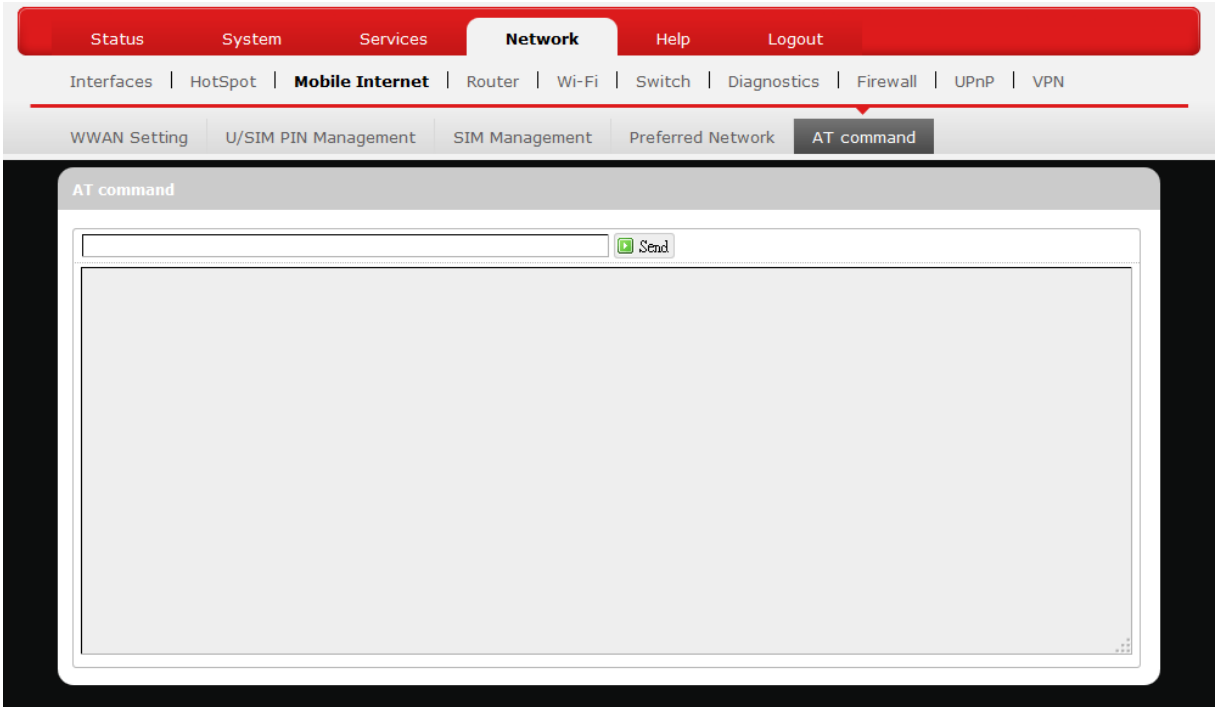


Preferred Network



Here you can select the preferred mobile network type by clicking and making a choice from the drop-down list. The available choice examples are Auto, *LTE* (4G), *CDMA* (3G), and *EVDO*.

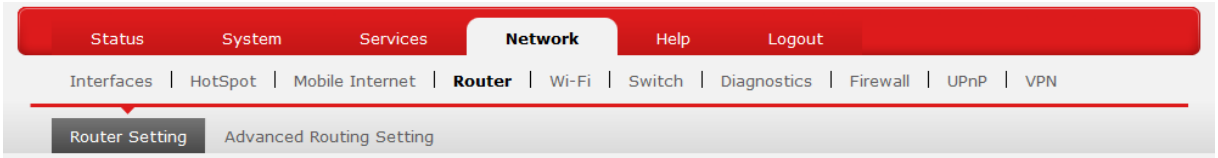
AT command



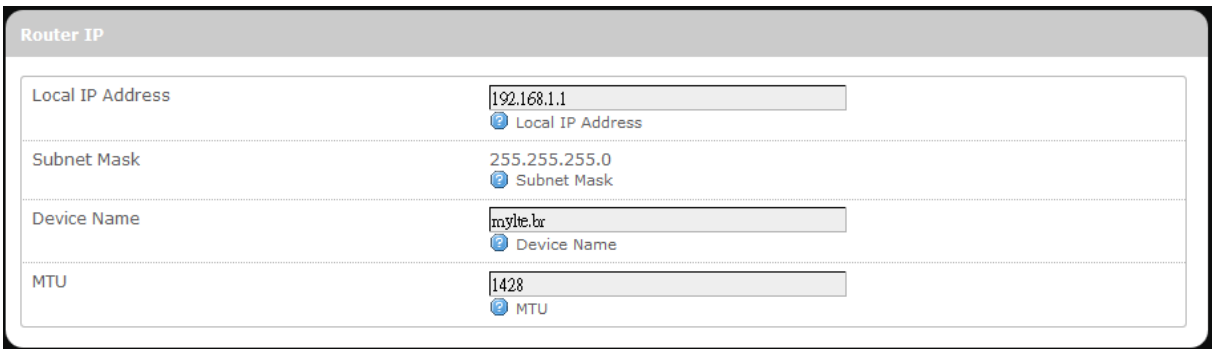
This section is for advanced users to control this router with the *AT command set* (also known as *Hayes command set)*. Enter each command in the text box and click Send .

Router

Router Settings

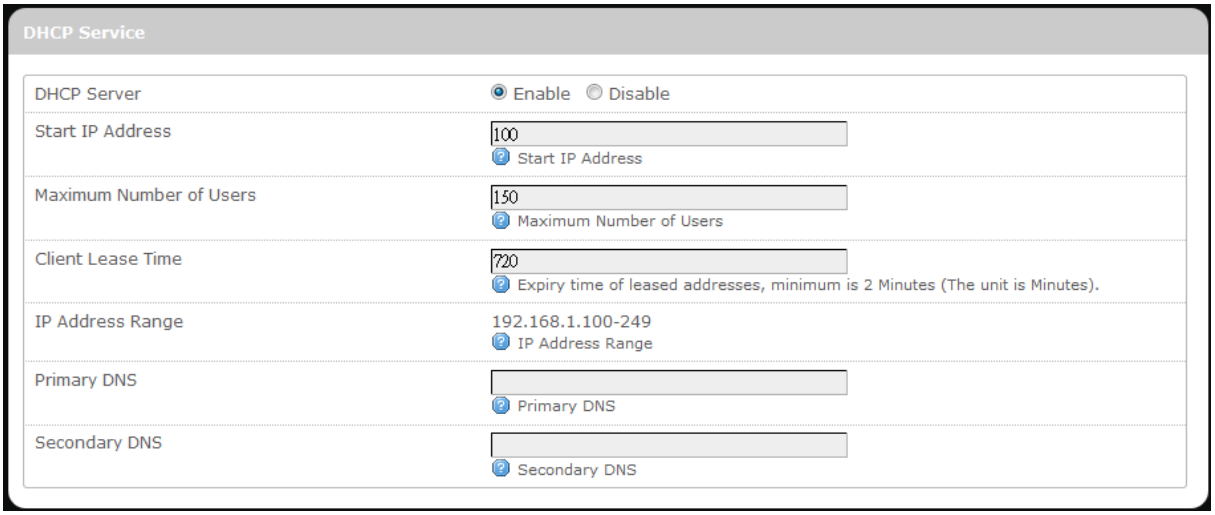


Router IP



Local IP Address:	If the default address conflicts with another local network device, you can enter another local IP address here.
Subnet Mask:	Displays current Subnet Mask
Device Name:	The device name can be changed by typing in the new device name in this text box.
MTU:	The MTU can be changed by typing in the new MTU value in this text box.

DHCP Service

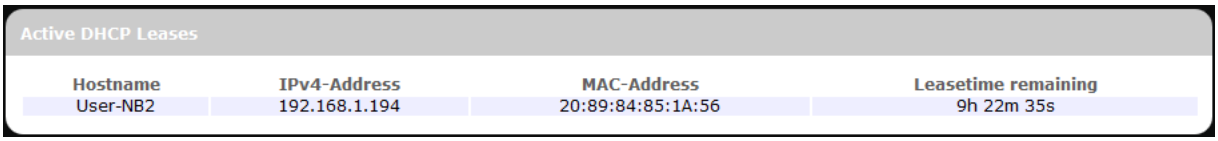


DHCP Server:	Enables or disables the DHCP Server feature.
Start IP Address:	Specifies the starting number of the last 3 digits of assigned client IP address. For example, the value of **100** means that the first assigned client IP address will be 192.168.1.**100**; the next assigned client IP address will be 192.168.1.**101**; and so on…
Maximum Number of Users:	Specifies maximum number of users for this router.
Client Lease Time:	Specifies the amount of lease time allocated to clients of this router, i.e. the expiry time of leased addresses.
IP Address Range:	Displays assignable local IP address range of this router

Primary DNS: If needed, specify the primary Domain Name System here.

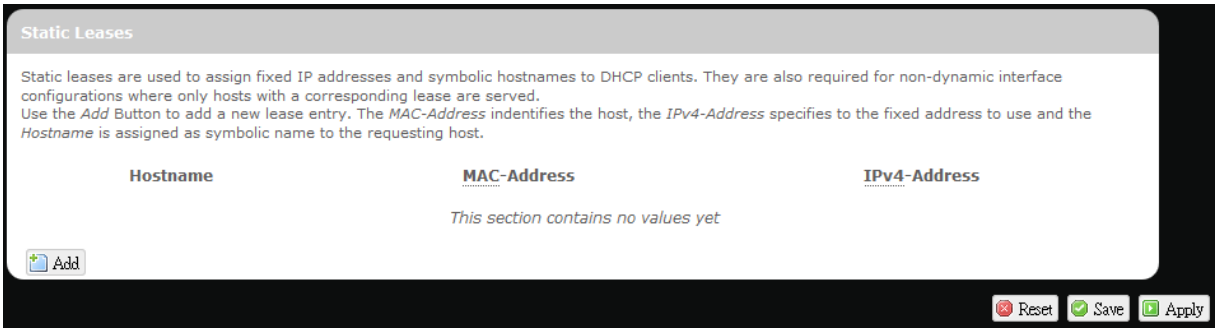
Secondary DNS: If needed, specify the secondary Domain Name System here.

Active DHCP Leases



This section displays active DHCP lease information for each client: **Hostname, IPv4 address**, **MAC address**, and **Lease time remaining**.

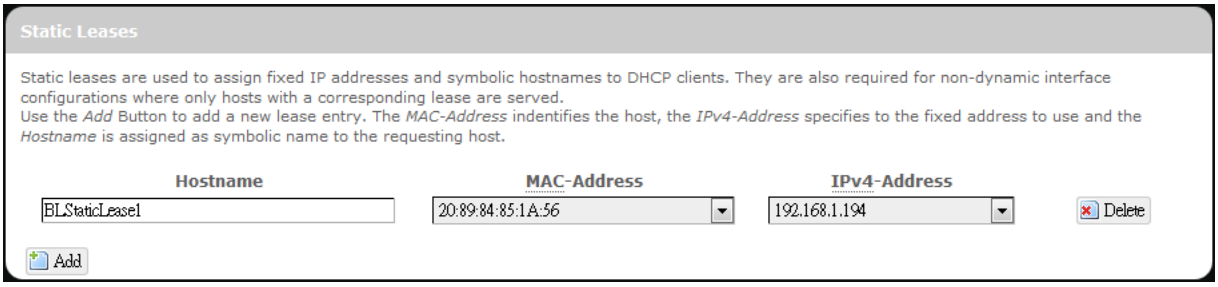
Static Leases


Static Leases
Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.
Use the Add Button to add a new lease entry. The MAC-Address indentifies the host, the IPv4-Address specifies to the fixed address to use and the Hostname is assigned as symbolic name to the requesting host.
Hostname
MAC-Address
IPv4-Address
This section contains no values yet
Add
Reset
Save
Apply

This option allows fixed IP address and symbolic hostname assignments for DHCP clients.

To add a static lease, first click

.


Static Leases
Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.
Use the Add Button to add a new lease entry. The MAC-Address indentifies the host, the IPv4-Address specifies to the fixed address to use and the Hostname is assigned as symbolic name to the requesting host.
Hostname
MAC-Address
IPv4-Address
BLStaticLease1
20:89:84:85:1A:56
192.168.1.194
Delete
Add

Enter the desired hostname. Choose the desired MAC address and IPv4-Address (click and select a rule from the drop-down list; if "--Custom--" is selected, the drop-down list will change to a text box to allow you to enter your custom address).

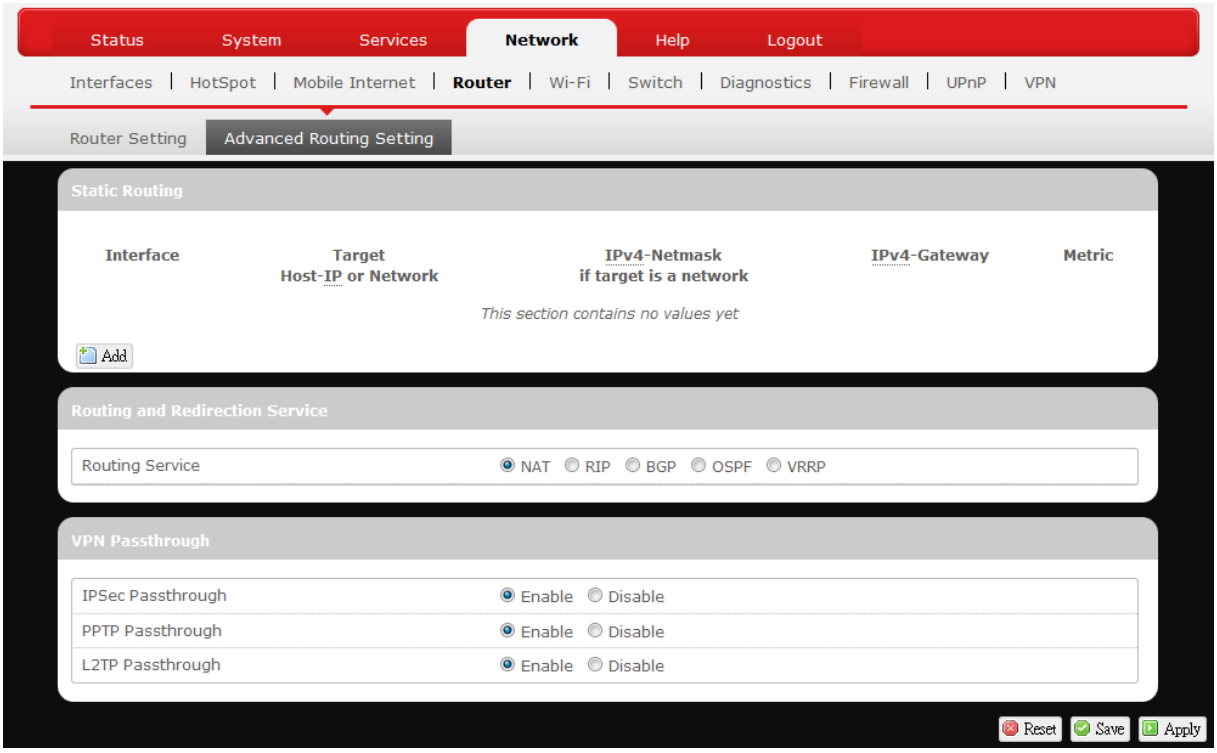
The MAC address is for host identification, whereas the IPv4 address specifies the fixed address for static lease.

To remove any unwanted static lease, just click the corresponding

Delete button.

Click Apply after making any changes.

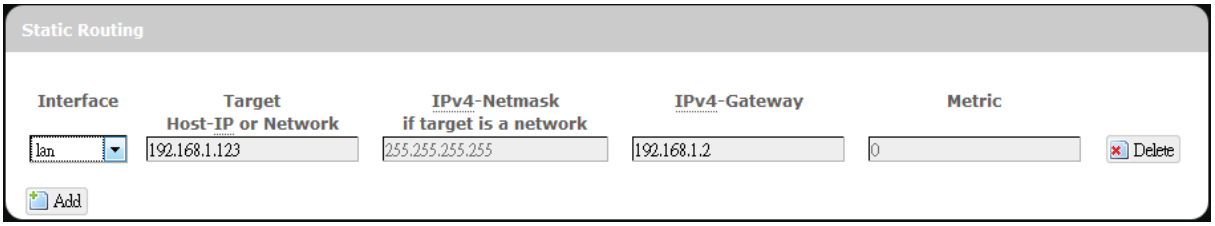
Advanced Routing settings



Static Routing

This option allows fixed network routing path assignment (as opposed to the initial adaptive routing).

To add a static network routing path, click Add. To remove any unwanted static network routing path, click the corresponding Delete button. Click Apply after making any changes.



Interface: Click and choose ‘lan’ (local area network), ‘wan’ (wide area network), or ‘wan2’ (wide area network 2).

Target: Enter the target host IP or network address here.

IPv4-Netmask:	Displays the IPv4-Netmask address. A custom IPv4-Netmask can also be specified here.
IPv4-Gateway:	If needed, a custom IPv4-Gateway address can be specified here.
Metric:	Specifies the network path priority number (usually associated with the network path's administrative distance). The lower the metric number, the higher priority of this static route in the network routing protocol. A different metric number can also be specified here.

Note: If contents in the text box is invalid, a will appear on the right side of the text box, and the text color changes to red. For example, the following demonstrates an invalid target Host-IP or Network address: 123.456.789.012

Routing and Redirection Service

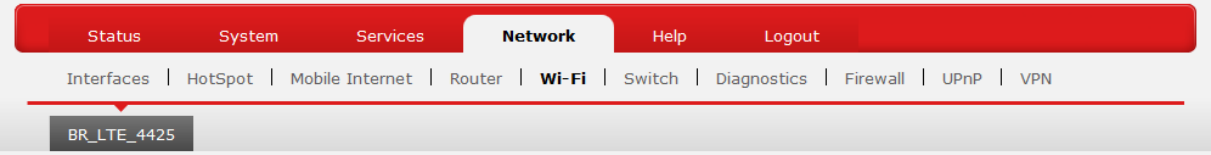
This option enables or disables Network Address Translation (NAT) service, which is a standard that allows multiple computers on a private network to share a single IP address.

VPN Passthrough

A Virtual Private Network (VPN) is a type of secured private network connection, built upon publicly-accessible infrastructure such as the Internet. They usually provide connectivity to various devices behind a gateway or firewall.

IPSec Passthrough:	IP Security (IPSec) provides authentication and encryption. Since it is mainly a Layer 3 technology, it can secure all data on the network. To allow IPSec tunnels to pass through the Router, click 'Enabled'.
PPTP Passthrough:	Point-to-Point Tunneling Protocol (PPTP) allows you to establish a connection to an enterprise network. To allow PPTP tunnels to pass through the Router, click Enabled.
L2TP Passthrough:	Layer 2 Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol and is also used to establish virtual private networks. To allow L2TP tunnels to pass through the Router, click Enabled.

WiFi



This submenu item is for configuring all Wi-Fi-related settings. This router initially has the default WiFi SSID. For example, the tab name "BR_LTE_xxxx" is the WiFi SSID.

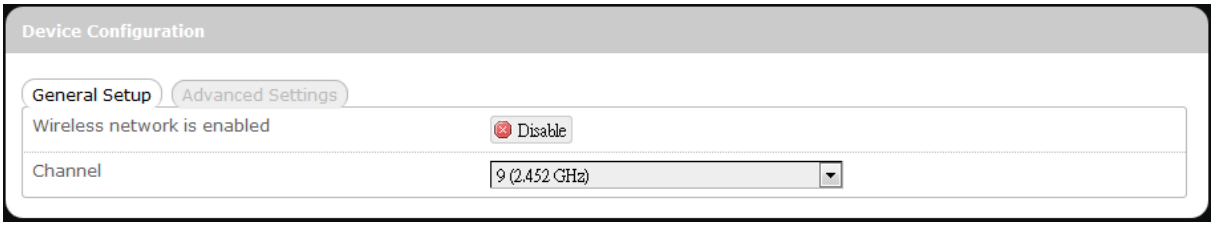
Note:

1. "xxxx" refers to the last four digits of this router's MAC address. For example, if the router's MAC address is 0026FA0B314A, then its corresponding SSID is BR_LTE_314A.
2. Initially this router has only the default SSID enabled. The *Dual SSID* feature can be enabled in the *Advanced Settings* tab under the setting *Device Configuration*.

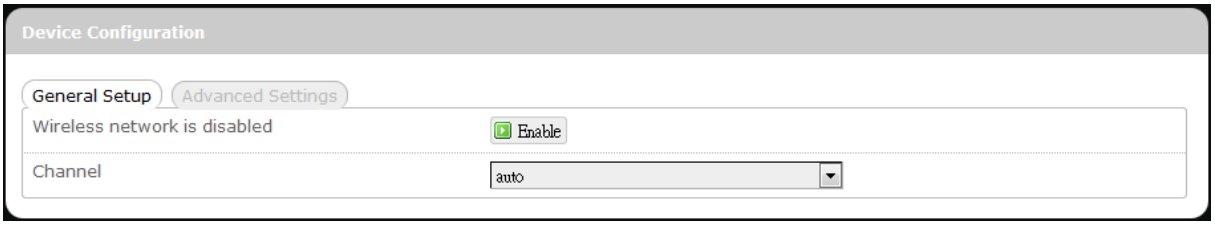
Please click Apply after making any changes in this submenu.

Device Configuration

General Setup

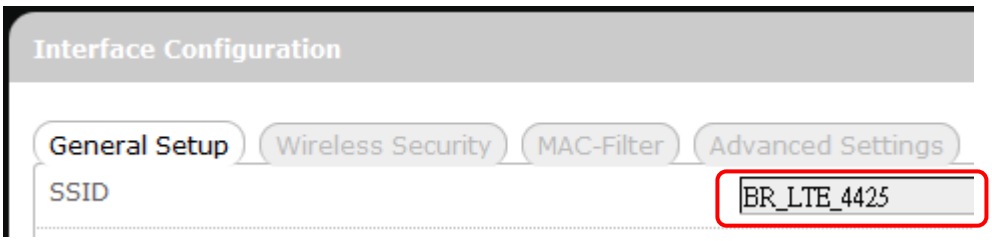


or



Wireless network is enabled*:	WiFi connection of the associated SSID is enabled. To disable WiFi connection of this SSID, click Disable.
Wireless network is disabled*:	WiFi connection of the associated SSID is disabled. To enable WiFi connection of this SSID, click Enable.

* Note: The associated SSID is displayed either in the selected submenu tab under WiFi or in the WiFi category item **Interface Configuration ➔ General Setup ➔ SSID**.

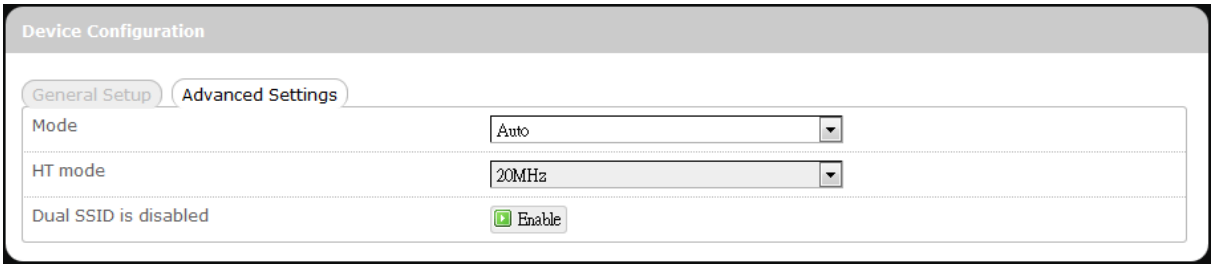


Channel: Selects the WiFi channel for communication. The available choices are:

Channel (carrier frequency)
1 (2.412 GHz)
2 (2.417 GHz)
3 (2.422 GHz)
4 (2.427 GHz)
5 (2.432 GHz)
6 (2.437 GHz)
7 (2.442 GHz)
8 (2.447 GHz)
9 (2.452 GHz)
10 (2.457 GHz)
11 (2.462 GHz)
auto ← assigns channel automatically

Normally one of the channels is already selected, and no change is needed unless there exists interference problems with other WiFi or Bluetooth devices (that also use the 2.4GHz frequency range for communications). Alternatively, you can select ‘auto’ to let the system select the channel automatically, or you can select “-- custom --” and enter your own channel specification in the text box.

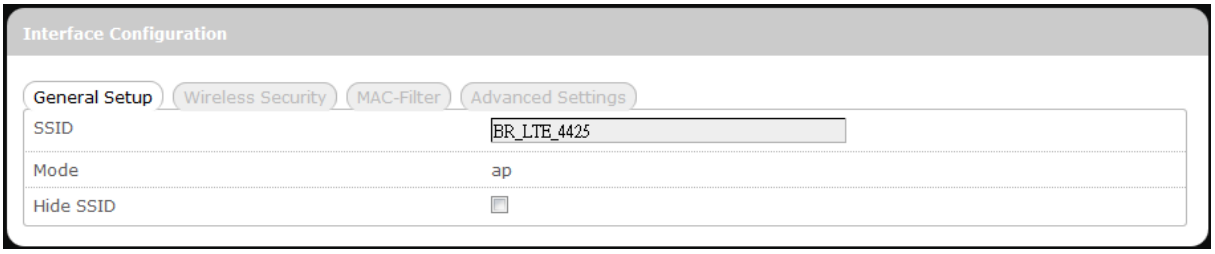
Advanced Settings



Mode	Specifies the IEEE wireless standard for WiFi communication. The choices are: Auto: The router automatically chooses the optimal IEEE wireless standard. 802.11b: Data speed up to 11 Mbps 802.11g: Data speed up to 54 Mbps 802.11n: Data speed up to 300 Mbps
HT mode	Specifies channel width for data communications. The choices are: 20MHz: Single 20MHz channel 20MHz / 40MHz Single or dual 20MHz channels
Dual SSID is disabled/enabled	Click Enable to activate the second SSID, or click Disable to deactivate the second SSID.

Interface Configuration

General Setup

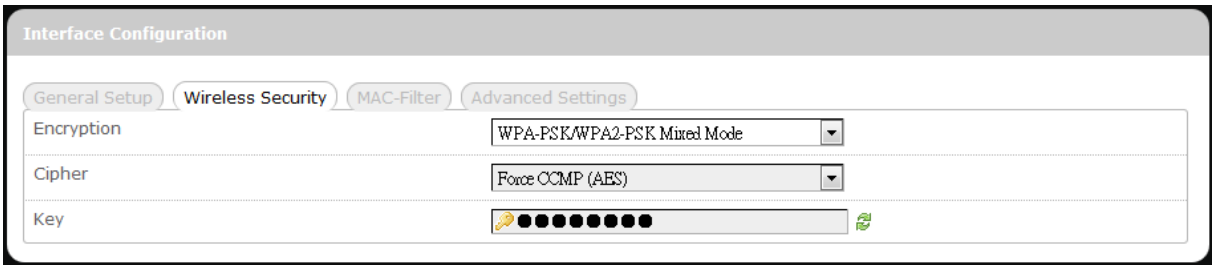


SSID	Service Set Identification To change the SSID, click the text box and enter the new SSID (up to 32 alphanumeric characters)
Mode	Wireless operating mode of this router. AP: Wireless Access Point
Hide SSID	Enable this option to make wireless network of *this* SSID unavailable to nearby WiFi clients.

Disable this option to make wireless network of *this* SSID available to nearby WiFi clients.

CAUTION: To enable “Hide SSID”, we strongly advise you to do so via wired LAN connection, since wireless LAN connection with this SSID will be lost with this option applied! If both SSIDs are hidden, then the communications with this router must be done via a LAN port, or this router must be reset to factory default settings.

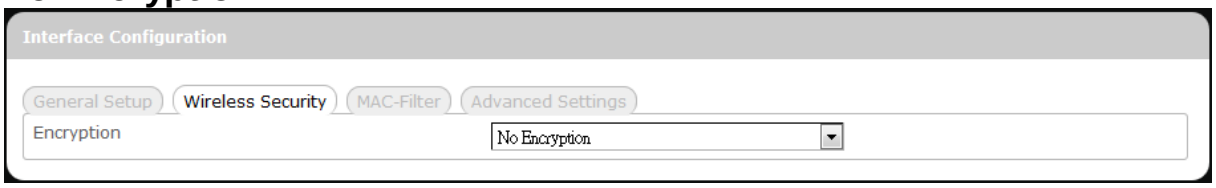
Wireless Security



This router supports wireless data encryption, a must for wireless data security. The Wireless Security Interface Configuration items will change according to the chosen encryption method.

The encryption options are:

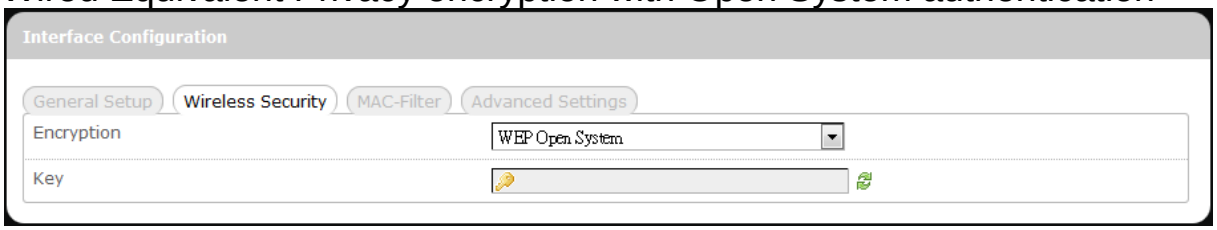
1. **No Encryption**



Data transmitted over wireless networks can be seen by others.

2. **WEP Open System**

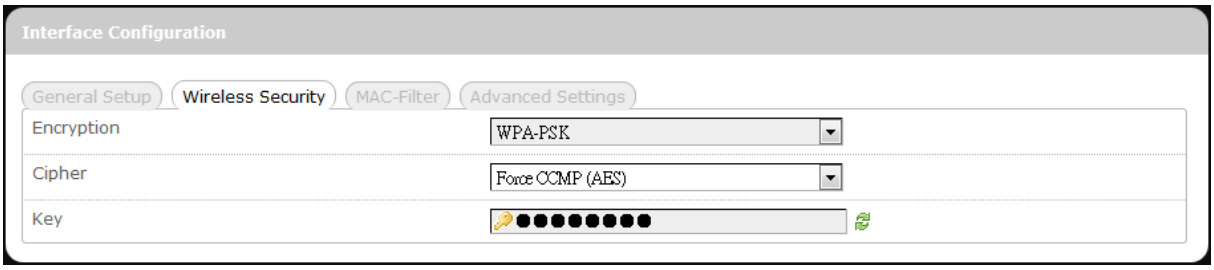
Wired Equivalent Privacy encryption with Open System authentication



Key: Enter a password for accessing this SSID’s wireless network.

3. **WPA-PSK**

“WiFi Protected Access – Pre-Shared Key” encryption



Cipher: Specify the desired encryption protocol by clicking and selecting an option from the drop-down list:

auto –the system automatically chooses the optimal encryption protocol

Force CCMP (AES) – Use CCMP (AES) encryption exclusively (stronger than TKIP)

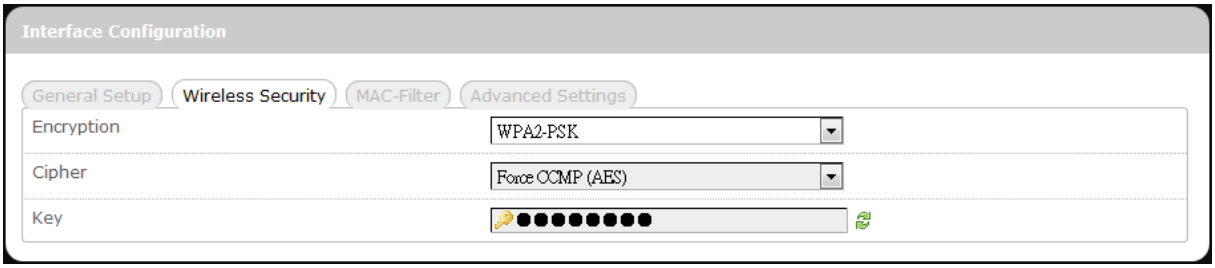
Force TKIP – Use TKIP encryption exclusively

Force TKIP and CCMP (AES) – Use TKIP and CCMP (AES) encryption protocols together

Key: Enter a password for accessing this SSID's wireless network.

4. **WPA2-PSK**

"WiFi Protected Access II – Pre-Shared Key" encryption



Cipher: Specifies the desired encryption protocol by clicking and selecting an option from the drop-down list:

auto –The system automatically chooses the optimal encryption protocol

Force CCMP (AES) – Use CCMP (AES) encryption exclusively (stronger than TKIP)

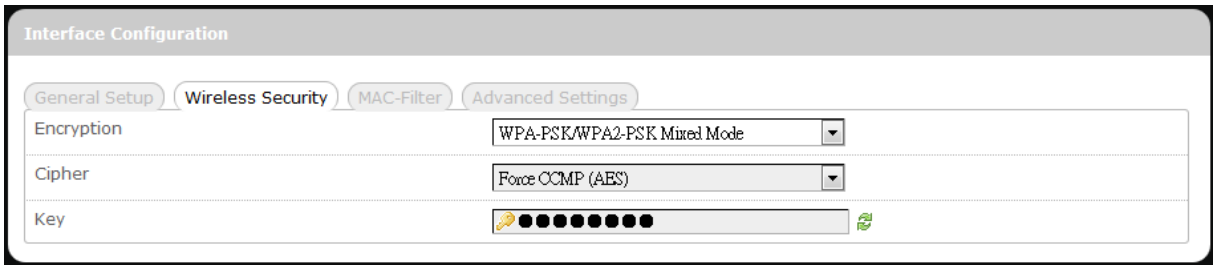
Force TKIP – Use TKIP encryption exclusively

Force TKIP and CCMP (AES) – Use TKIP and CCMP (AES) encryption protocols together

Key: Enter a password for accessing this SSID's wireless network.

5. **WPA-PSK/WPA2-PSK Mixed Mode**

"WiFi Protected Access I + II – Pre-Shared Key" encryption



Cipher: Specifies the desired encryption protocol by clicking and selecting an option from the drop-down list:

auto – The system automatically chooses the optimal encryption protocol

Force CCMP (AES) – Use CCMP (AES) encryption exclusively (stronger than TKIP)

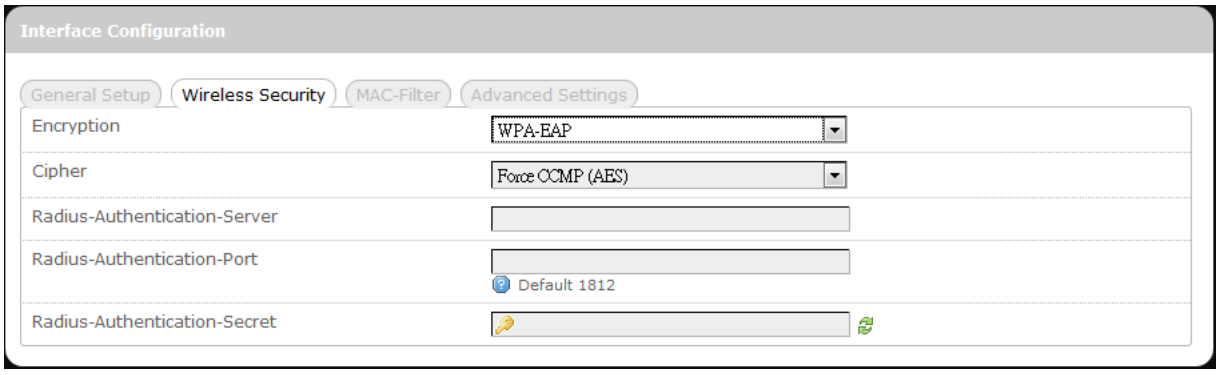
Force TKIP – Use TKIP encryption exclusively

Force TKIP and CCMP (AES) – Use TKIP and CCMP (AES) encryption protocols together

Key: Enter a password for accessing this SSID's wireless network.

6. **WPA-EAP**

"WiFi Protected Access – Extensible Authentication Protocol" encryption



Cipher: Specifies the desired encryption protocol by clicking and selecting an option from the drop-down list:

auto – The system automatically chooses the optimal encryption protocol

Force CCMP (AES) – Use CCMP (AES) encryption exclusively (stronger than TKIP)

Force TKIP – Use TKIP encryption exclusively

Force TKIP and CCMP (AES) – Use TKIP and CCMP (AES) encryption protocols together

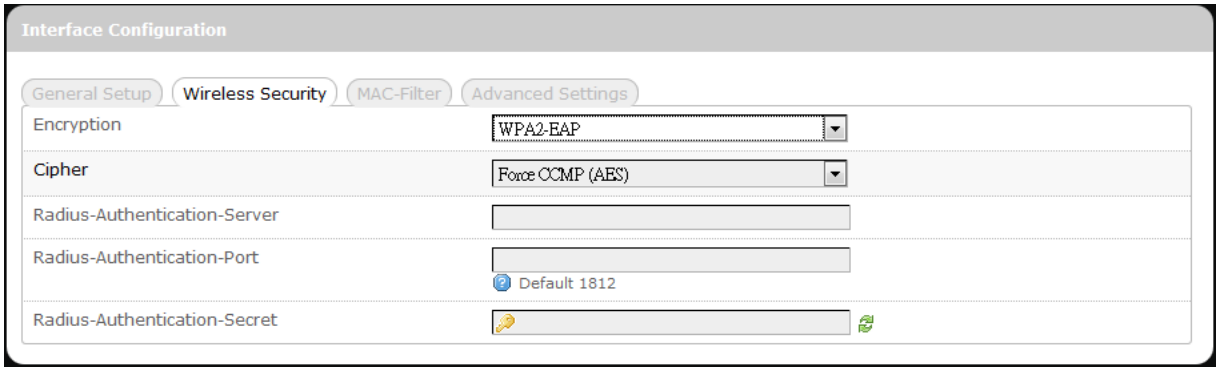
Radius-Authentication-Server: Enter the name of the RADIUS authentication server.

Radius-Authentication-Port: Enter the port number of the RADIUS authentication port.

Radius-Authentication-Secret: Enter the desired RADIUS secret password.

7. **WPA2-EAP**

"WiFi Protected Access II – Extensible Authentication Protocol" encryption



Cipher: Specifies the desired encryption protocol by clicking and selecting an option from the drop-down list:

auto – The system automatically chooses the optimal encryption protocol

Force CCMP (AES) – Use CCMP (AES) encryption exclusively (stronger than TKIP)

Force TKIP – Use TKIP encryption exclusively

Force TKIP and CCMP (AES) – Use TKIP and CCMP (AES) encryption protocols together

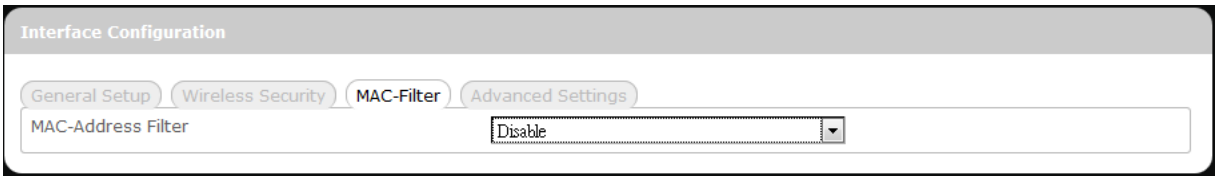
Radius-Authentication-Server: Enter the name of the RADIUS authentication server.

Radius-Authentication-Port: Enter the port number of the RADIUS authentication port.

Radius-Authentication-Secret: Enter the desired RADIUS secret password.

MAC-Filter

MAC-Address Filter:

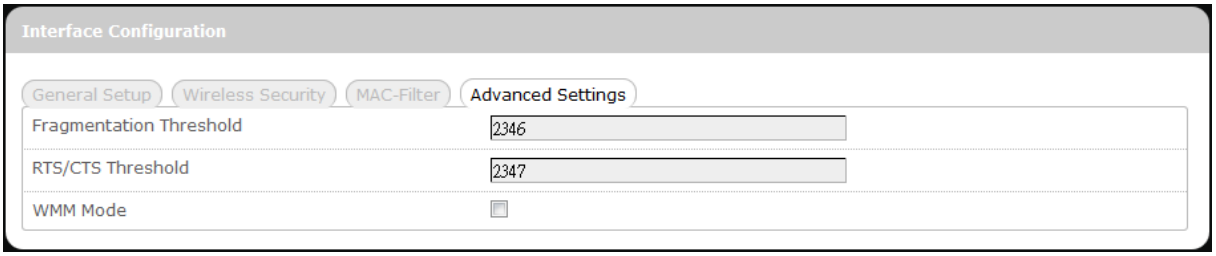


This tab item allows you to selectively allow or block clients from network access. Click ▣ and select an option from the drop-down list:

1. Disable – The MAC address filter is disabled.
2. White list* – Click ▣ and select a desired MAC address from the drop-down list, or select “-- custom --" and enter a specific client’s MAC address.
3. Black list* – Click ▣ and select an undesired MAC address from the drop-down list, or select “-- custom --" and enter a specific client’s MAC address.

* To add another MAC address to the list, click 🗋 to add a new drop-down list; then repeat the MAC address selection/specification. To remove a MAC address from the list, click ✖.

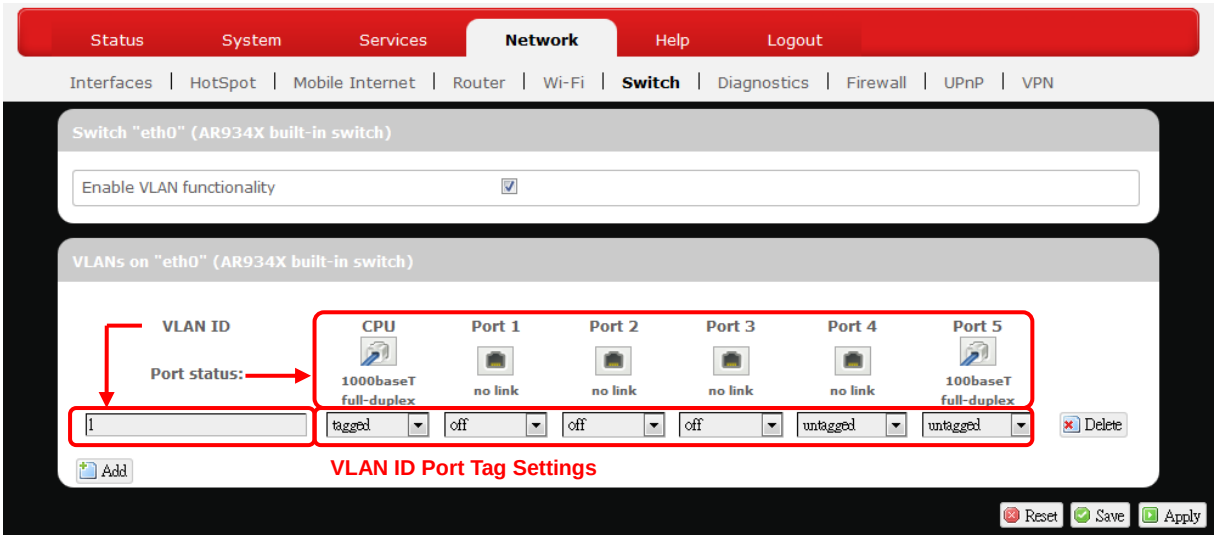
Advanced Settings



This tab item is for advanced adjustment settings for WiFi connection.

Fragmentation Threshold:	Maximum transmittable data packet frame size without frame fragmentation.
RTS/CTS Threshold:	Defines Request-To-Send (transmitter) and Clear-To-Send (receiver) control packet size.
WMM Mode:	Enables or disables Wi-Fi Multimedia Mode, which gives multimedia data contents (voice, video, and audio) higher priority over wireless networks.

Switch



This submenu is for advanced users to view and configure this router's VLAN (Virtual Local Area Network) status and tag settings. The use of different VLAN IDs, each with its own tag settings for each logical network port, allows the router's network to be partitioned into different virtual networks (up to 4095).

Switch "eth0" (AR934X built-in switch)

Enable VLAN functionality: Here you can enable or disable the VLAN feature.

VLAN on "eth0" (AR934X built-in switch)

VLAN ID: Enter the desired VLAN Identification Number here (1-4094). Different VLAN IDs have different roles and functions. Click Add to set up another VLAN ID and its tag settings, or click Delete to remove a particular VLAN ID.

0: Reserved for tagging priority of data packets. This VLAN ID is not available for the user.

1-511: Reserved for normal VLANs.

512-4094: Reserved for VLAN *circuit cross-connect (CCCs)*.

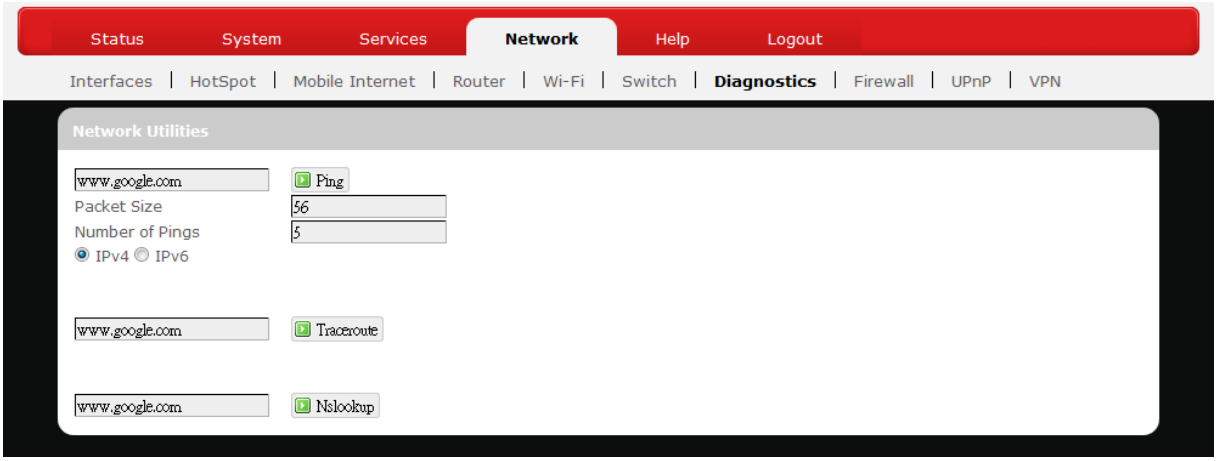
Port status:	Displays the name, the symbolic icon, and the connection status for each of the logical network ports (here we have six of them: *CPU* and *Port 1-5*). The connection status for each logical network port is defined as follows:	
	no link:	No network connection is established.
	1000baseT full-duplex:	Network connection is established at 1000 Mbps.
	1000baseT full-duplex:	Network connection is established at 100 Mbps.
VLAN ID Port Tag Settings:	This row of settings allows you to define the tagging status for each logical network port within a particular VLAN ID.	
	Off	Each *packet* flowing through the associated network port does not belong to *this* VLAN ID.
	Untagged:	Each *packet* flowing through the associated network port belongs to the default VLAN ID (VLAN 0).
	Tagged:	Each *packet* (sometimes known as *Ethernet frame)* flowing through the associated network port belongs specifically to *this* VLAN ID.

To make changes in this submenu effective, click

.

Note:	*A packet* is an unit of network data and is sometimes known as an *Ethernet frame* or a *frame*.

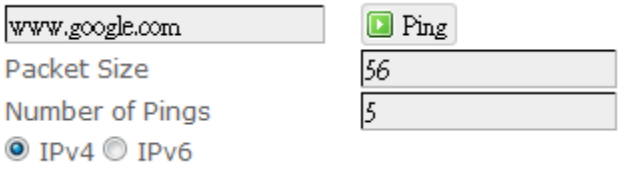
Diagnostics



This submenu contains tools for effective network analysis and troubleshooting.

Network Utilities

Ping



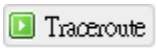
This feature allows you to check the status of a connection.

1. In the text box next to Ping, enter the IP address or URL that you want to ping, and then select its corresponding internet protocol by clicking either the IPv4 or IPv6 radial button.
2. In the text box of “Packet Size”, enter the desired value.
3. In the text box of “Number of Pings”, enter the number of times you wish to ping.
4. Click Ping to begin the connection status check. ‘Ping’ messages will appear below.

Traceroute

This feature allows you to check the performance of a connection.

1. In the text box next to

, enter the IP address or URL that you want to trace route, and then click 

to start the performance text. ‘Traceroute’ messages will appear below.

NS Lookup

This feature allows you to retrieve name server information.

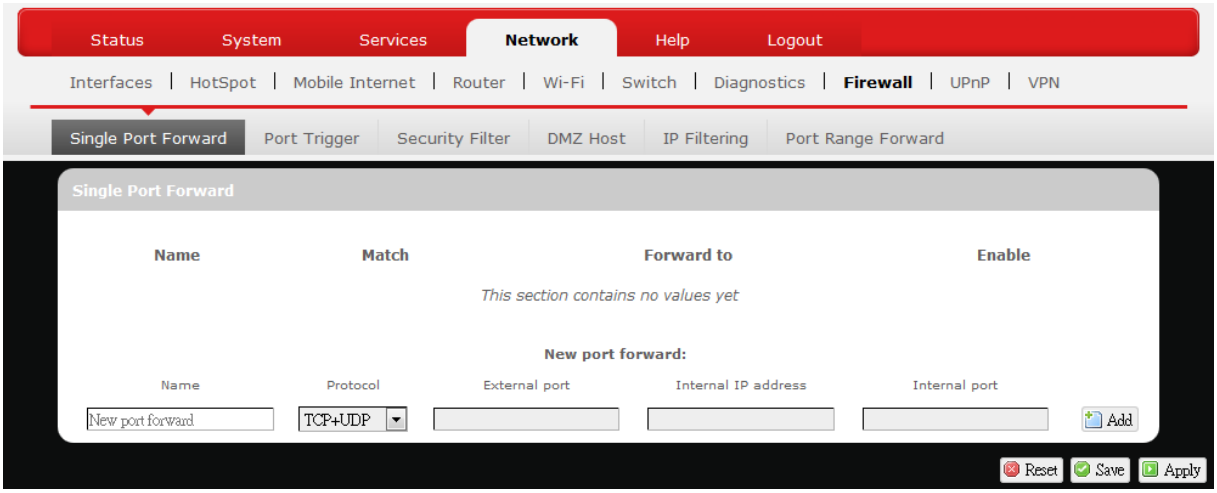
1. In the text box next to

, enter the IP address or URL that you want to trace route, and then click

to get name server information. ‘Nslookup’ messages will appear below.

Firewall

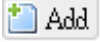
Single Port Forward

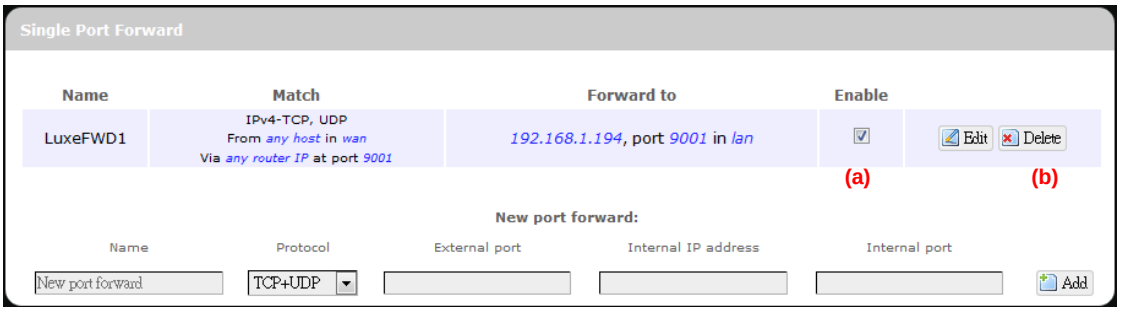


Single Port Forward

Port Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, and other specialized Internet applications.

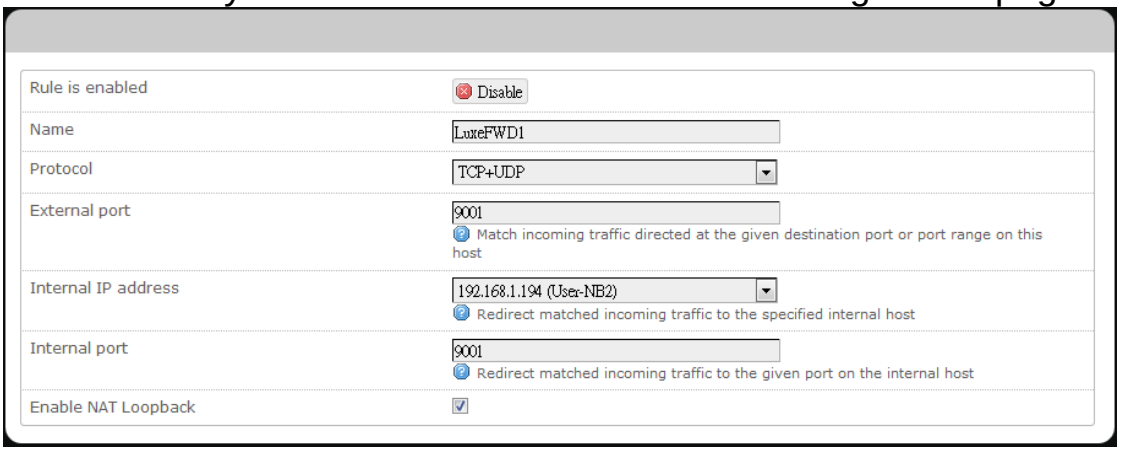
To forward a single port:

1. **Name**: Enter an application name for this port forwarding rule.
2. **Protocol**: Click and select a protocol from the drop down list – *TCP+UDP*, *TCP*, *UDP*.
3. **External port**: Enter the port number of the external port used by the server or Internet application. Afterward, this port number will be echoed to the text box of “Internal port”.
4. **Internal IP address**: Enter IP address in text box.
5. **Internal port**: This text box will automatically receive port number entered in the text box of “External port”, or you can enter your own port number in the same text box.
6. Click  . The port forwarding rule you have just entered will be added to the Port Forwards list.



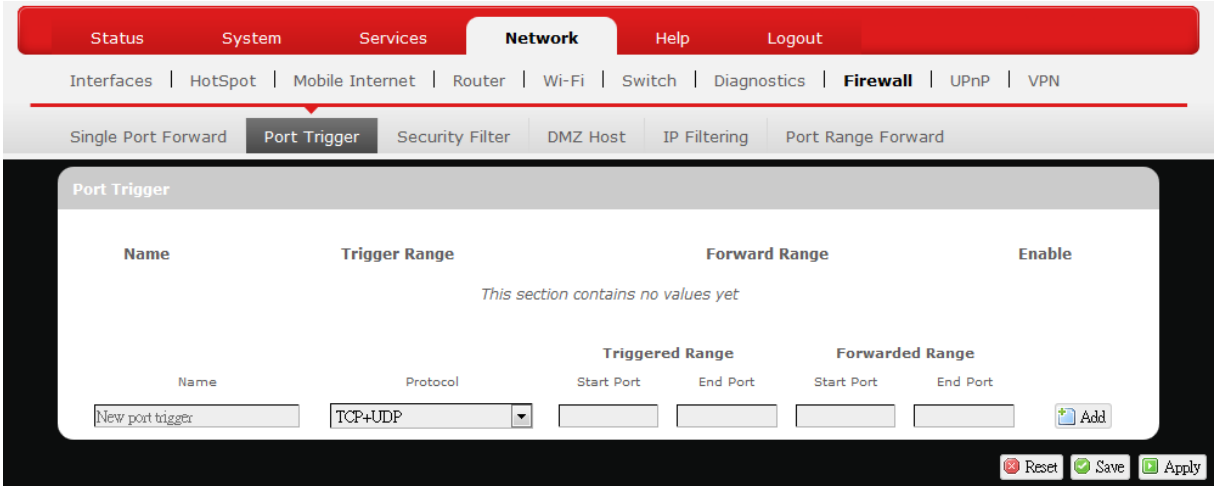
In the status area, the message **Unapplied Change** may appear next to “Operator Name” to indicate configuration changes temporarily stored in the router.

7. More rules can be added to the Port Forwards list by repeating Steps 1-6.
8. (a)To enable or disable a Port Forwards list rule, click its check box under ‘Enable’.
   (b) To remove any Port Forwards rule, click its corresponding Delete button.
9. To edit a particular Port Forwards rule in detail, click its corresponding Edit button, and the rule’s associated configuration page (much more flexible and detailed than express settings in Steps 1-5) will appear. After making any changes, click Apply. Finally click Back to Overview to exit this configuration page.



Note:	Numerical and text values shown in the illustrative examples are for demonstration purposes only and are not for actual operation.

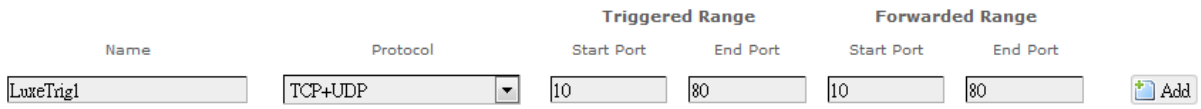
Port Trigger



Port Trigger

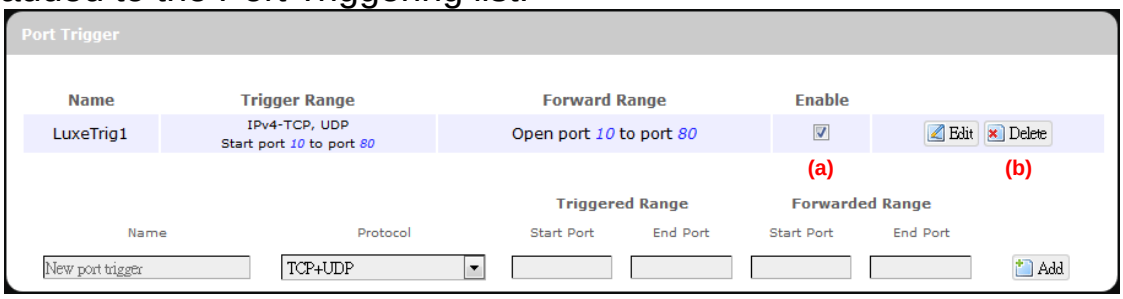
Port Triggering allows the Router to watch outgoing data for specific port numbers. The Router remembers the IP address of the computer that sends the matching data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

To add a new Port Triggering rule:



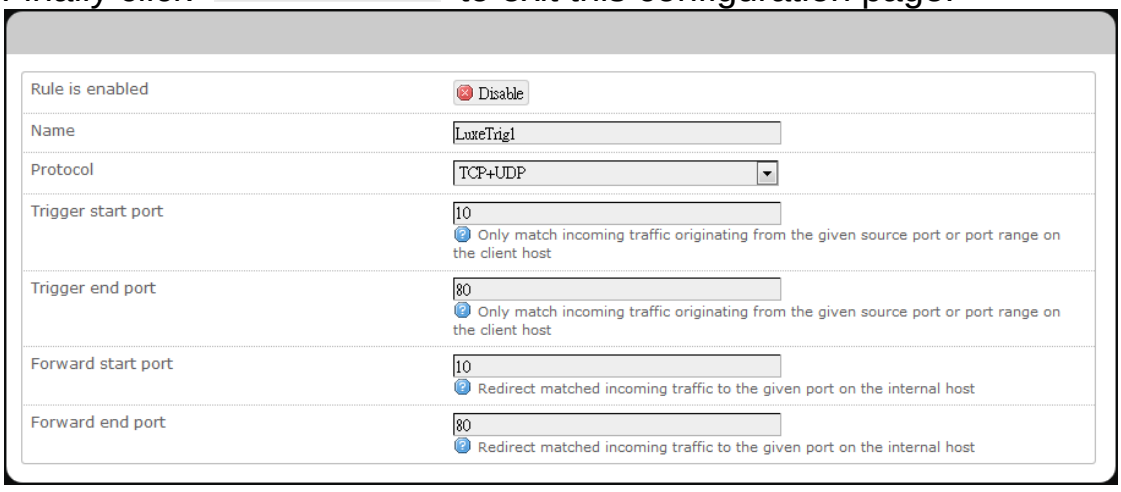
1. **Name**: enter an application name for this port triggering rule.
2. **Protocol**: click and select a protocol from the drop down list – *TCP+UDP*, *TCP*, *UDP*.
3. **Triggered Range**: enter the **Start Port** and **End Port** for the triggered port number range of the Internet application (please check its documentation for the port number(s) needed).
4. **Forwarded Range**: enter the **Start Port** and **End Port** for the forwarded port number range of the Internet application (please check its documentation for the port number(s) needed).

5. Click Add. The port triggering rule you have just entered will be added to the Port Triggering list.



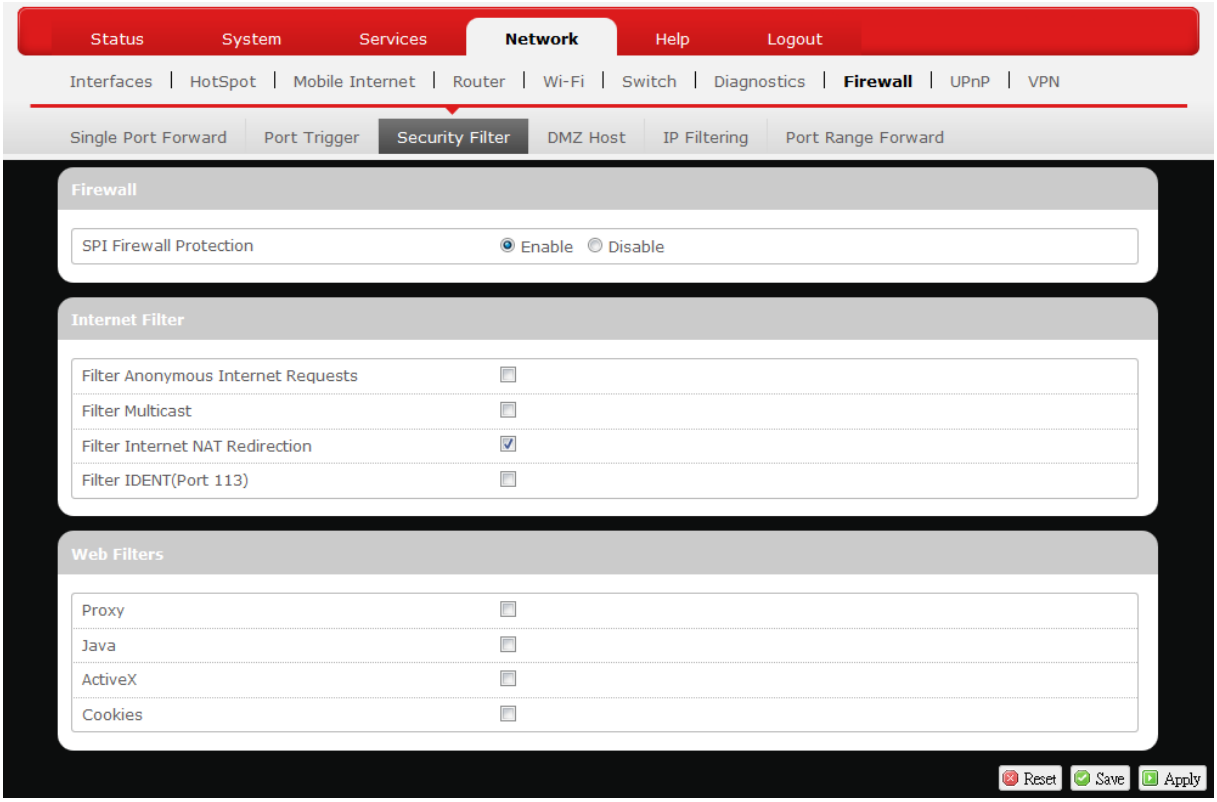
In the status area, the message **Unapplied Change** may appear next to "Operator Name" to indicate configuration changes stored in the router.

6. More rules can be added to the Port Triggering list by repeating Steps 1-5.
7. (a) To enable or disable a Port Forwards list rule, click its check box under 'Enable'.
   (b) To remove any Port Triggering rule, click its corresponding Delete button.
8. To edit a particular Port Triggering rule in detail, click its corresponding Edit button, and the rule's associated configuration page (more flexible and detailed than express settings in Steps 1-4) will appear. After making any changes, click Apply. Finally click Back to Overview to exit this configuration page.


Rule is enabled
Disable
Name
LuxeTrig1
Protocol
TCP+UDP
Trigger start port
10
Only match incoming traffic originating from the given source port or port range on the client host
Trigger end port
80
Only match incoming traffic originating from the given source port or port range on the client host
Forward start port
10
Redirect matched incoming traffic to the given port on the internal host
Forward end port
80
Redirect matched incoming traffic to the given port on the internal host

Note: Numerical and text values shown in the illustrative examples are for demonstration purposes only and are not for actual operation.

Security Filter



Here you can make **Firewall**, **Internet Filter**, and **Web Filters** adjustments for network security.

Firewall

SPI Firewall Protection: Enable or Disable Stateful Packet Inspection (SPI) feature of the firewall.

Internet Filter

Filter Anonymous Internet Requests: This filter blocks anonymous internet requests from outside network.

Filter Multicast: Multicasting allows for multiple transmissions to specific recipients at the same time, i.e. the Router allows IP multicast packets to be forwarded to the appropriate computers.

To allow multicasting, disable “Filter Multicast” .

To block multicasting, enable “Filter Multicast”.

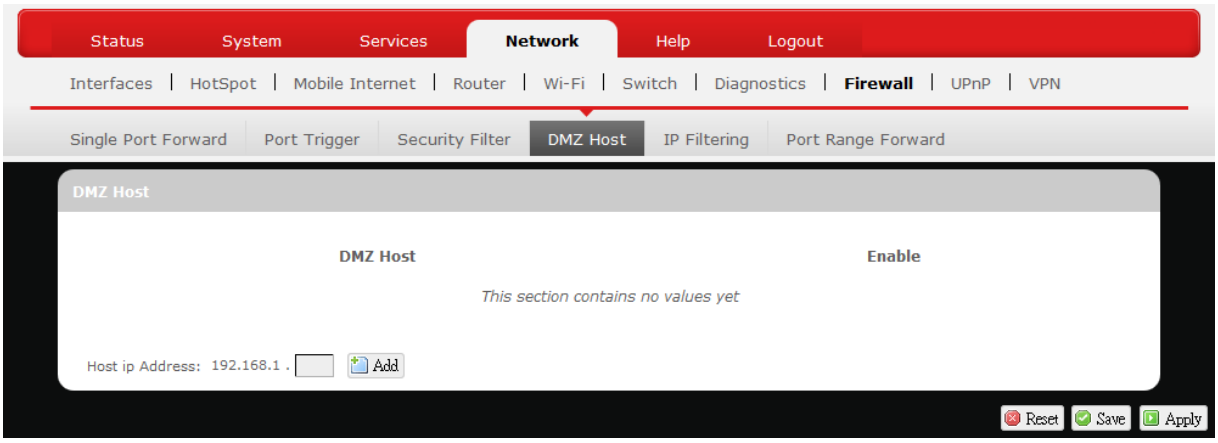
Filter Internet NAT Redirection:	This filter blocks local resource access via NAT (Network Address Translation) redirection (i.e. external address) from other local computers.
Filter IDENT (Port113):	This feature keeps Port 113 from being scanned by devices outside of your local network.

Web Filters

Using the Web Filters feature, you may enable up to four specific filtering methods.

Proxy:	Use of WAN proxy servers may compromise the Router's security. Select this option to disable access to any WAN proxy servers.
Java:	Java is a programming language for websites. Select this option to disable Java. If you disable Java, you run the risk of not having access to Internet sites created using this programming language.
ActiveX:	ActiveX is a programming language for websites. Select this option to disable ActiveX. If you disable ActiveX, you run the risk of not having access to Internet sites created using this programming language.
Cookies:	A cookie is data stored on your PC and used by Internet sites when you interact with them. Select this option to disable cookies.

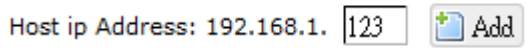
DMZ Host



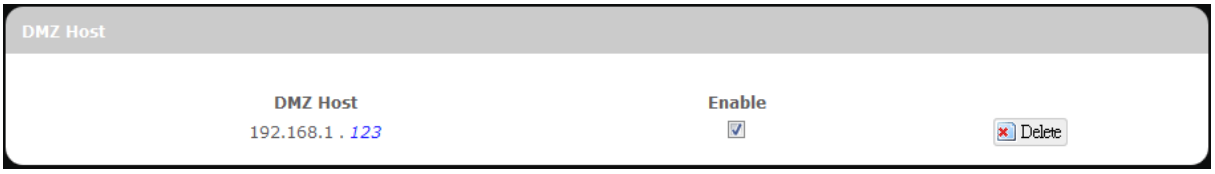
When a firewall is used, it is sometimes necessary to place some clients

(for example Internet games, video conferencing, or VPN connections) outside of the firewall while leaving the others protected. You can do this using a Demilitarized Zone (DMZ). This DMZ Host feature allows you to specify the IP address of the computers that are placed outside the firewall of your network.

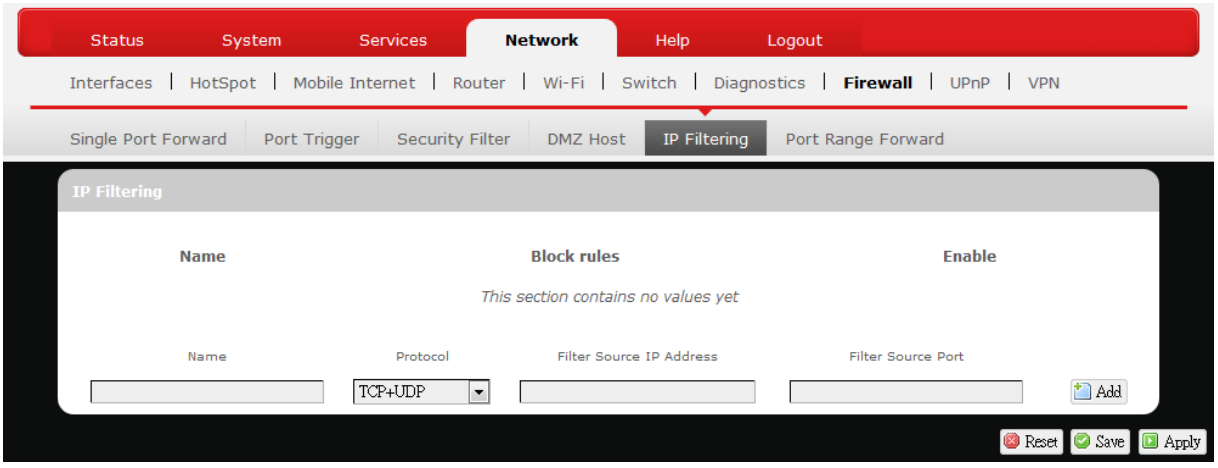
In the text box, enter the last 3 digits of the DMZ host address (the prefix is 192.168.1 for this router), and then click Add.



The host IP address will be added to the DMZ Host list, which can be further disabled or enabled by clicking the 'Enable' checkbox. To remove this DMZ Host, click Delete. After setting up the DMZ host, click Apply.



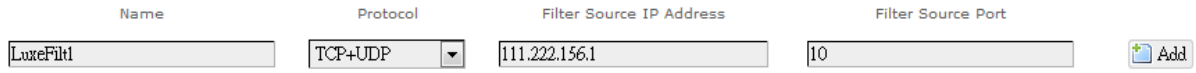
IP Filtering



IP Filtering

IP Filtering allows the Router to discard data from certain IP addresses.

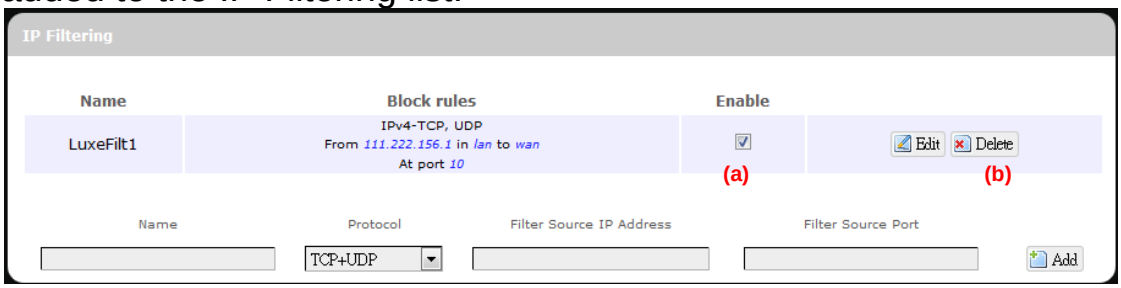
To add a new IP filtering rule:



1. **Name**: Enter an application name for this IP filtering rule.
2. **Protocol**: Click and select a protocol from the drop down list – *TCP+UDP*, *TCP*, *UDP*.
3. **Filter Source IP Address**: Enter the source IP address to be

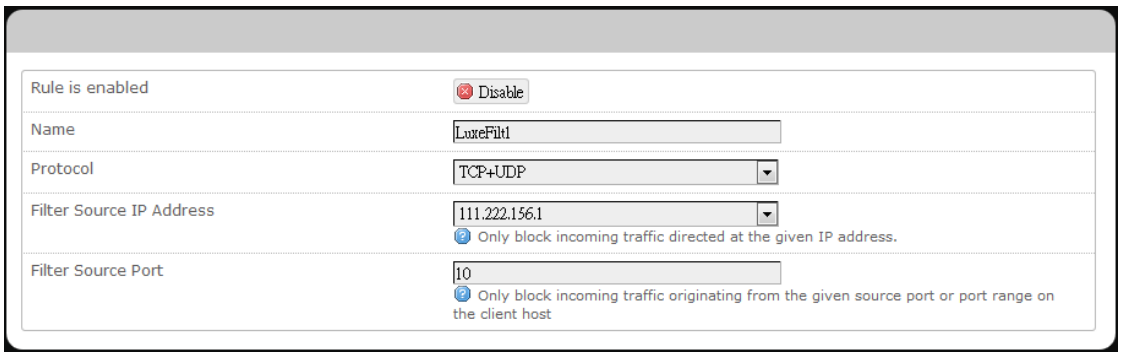
filtered. The text color will turn red with on the right for any invalid IP address entered (e.g. 192.168.234.). When the IP address entered becomes valid, the text color changes back to black without on the right (e.g. 192.168.234.5).

4. **Filter Source Port**: Enter the source port number to be filtered.
5. Click Add. The IP filtering rule you have just entered will be added to the IP Filtering list.



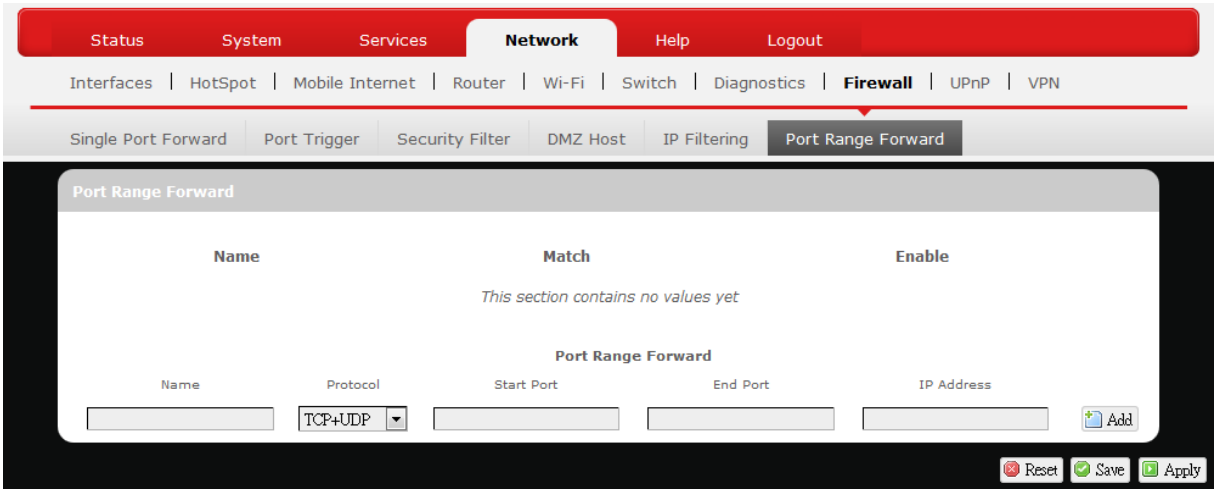
In the status area, the message **Unapplied Change** may appear next to “Operator Name” to indicate configuration changes stored in the router.

6. More rules can be added to the IP filtering list by repeating Steps 1-5.
7. (a) To enable or disable an IP filtering list rule, click its check box under ‘Enable’.
   (b) To remove any Port Triggering rule, click its corresponding Delete button.
8. To edit a particular IP filtering rule in detail, click its corresponding Edit button, and the rule’s associated configuration page (more flexible and detailed than express settings in Steps 1-4) will appear. After making any changes, click Apply. Finally click Back to Overview to exit this configuration page.



Note:	Numerical and text values shown in the illustrative examples are for demonstration purposes only and are not for actual operation.

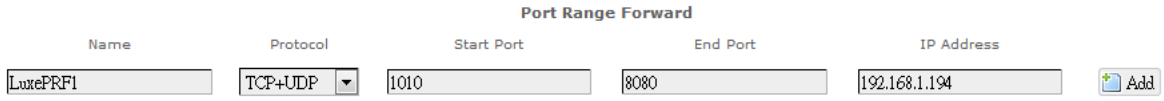
Port Range Forward



Port Range Forward

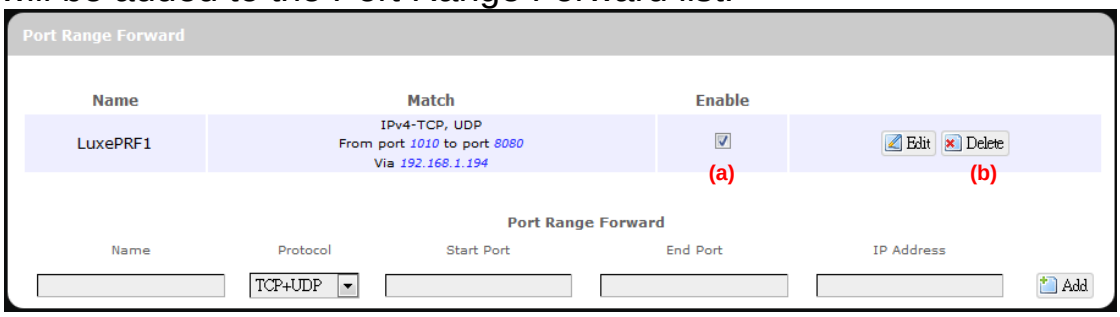
Port Range Forward allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, and other specialized Internet applications.

To forward a port range:



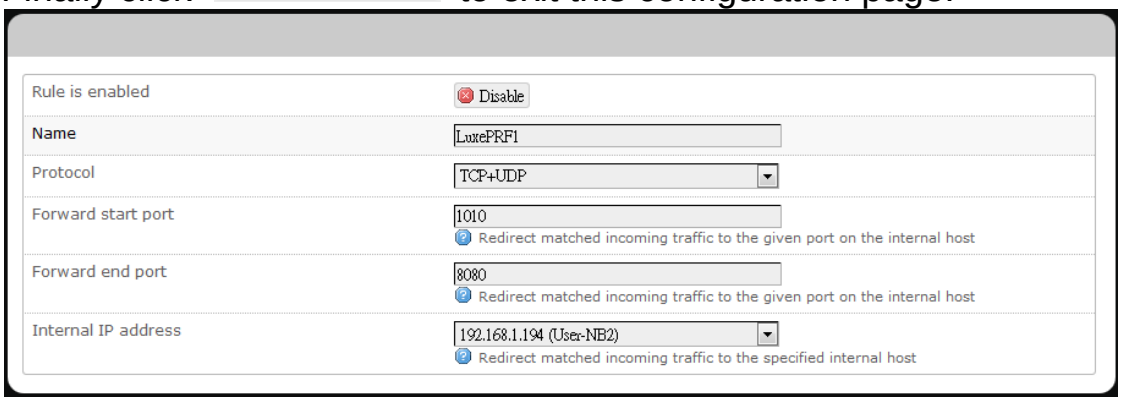
1. **Name**: Enter an application name for this port range forwarding rule.
2. **Protocol**: Click ▼ and select a protocol from the drop down list – *TCP+UDP*, *TCP*, *UDP*.
3. **Port Range Forward**: Specify the range of port forwarding by entering the **Start Port** number and the **End Port** number.
4. **IP address**: Enter the IP address of the PC running the specific application.

5. Click Add. The port range forwarding rule you have just entered will be added to the Port Range Forward list.



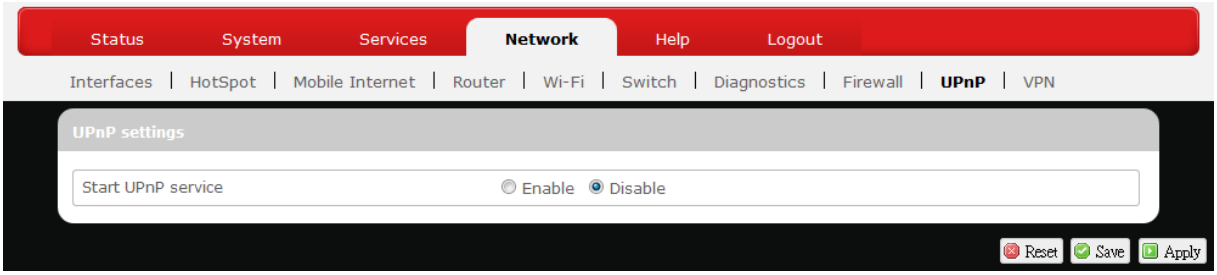
In the status area, the message **Unapplied Change** may appear next to "Operator Name" to indicate configuration changes temporarily stored in the router.

6. More rules can be added to the Port Range Forward list by repeating Steps 1-5.
7. (a) To enable or disable a Port Forwards list rule, click its check box under 'Enable'.
   (b) To remove any Port Forwards rule, click its corresponding Delete button.
8. To edit a particular Port Forwards rule in detail, click its corresponding Edit button, and the rule's associated configuration page (more flexible and detailed than express settings in Steps 1-4) will appear. After making any changes, click Apply. Finally click Back to Overview to exit this configuration page.



Note:	Numerical and text values shown in the illustrative examples are for demonstration purposes only and are not for actual operation.

UPnP

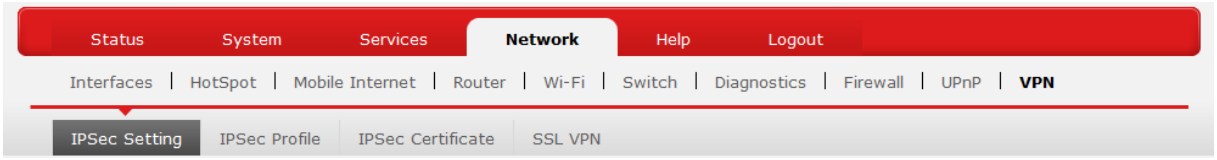


Universal Plug and Play – Allows wired and wireless network devices to discover each other and establish network services.

UPnP Settings

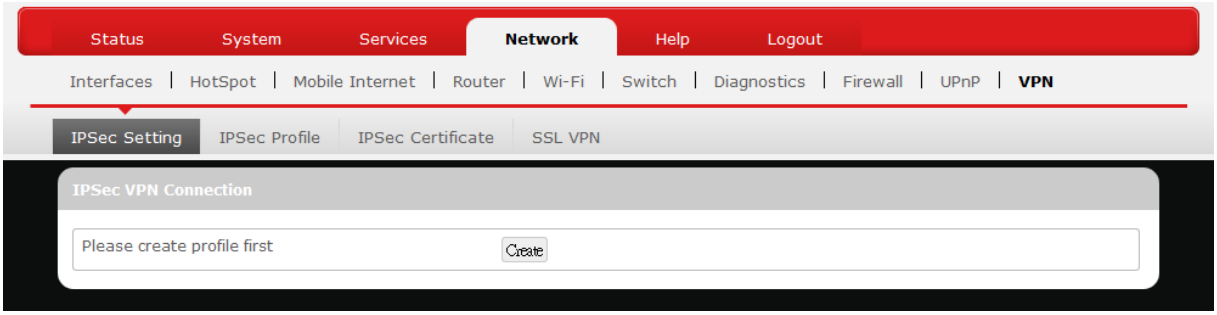
Here you can ‘Enable’ or ‘Disable’ the UPnP service.

VPN



Virtual Private Network – Allows use of mobile internet for secured private network.

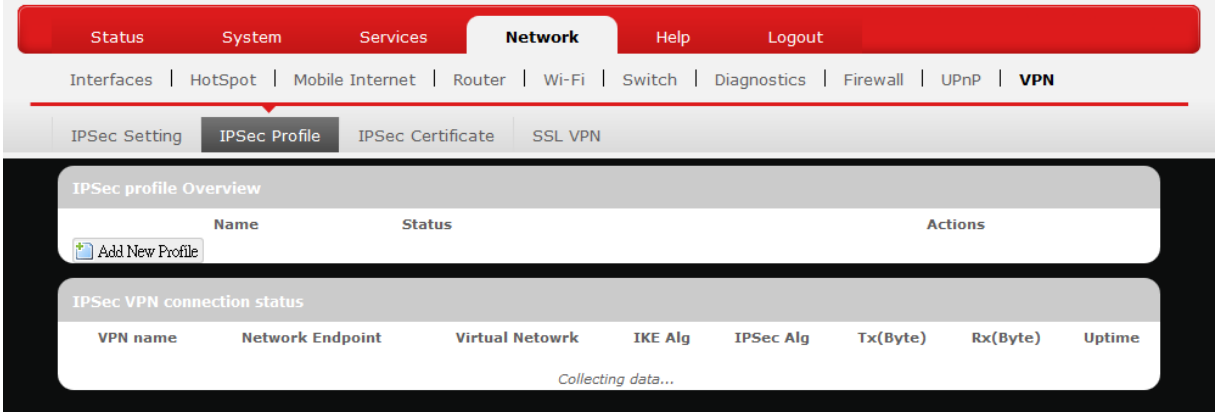
IPSec Setting



IPSec VPN Connection

First click **Create** to create a profile, then follow subsequent instructions.

IPSec Profile



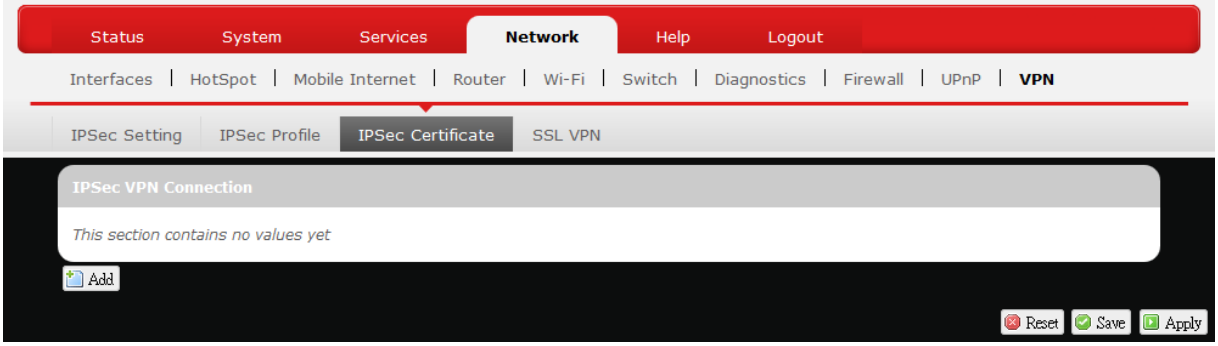
IPSec profile Overview

First click **Add New Profile** to create a profile, then follow subsequent instructions.

IPSec VPN connection status

Here you can view the status of VPN connection. The displayed information are **VPN name**, **Network Endpoint**, **Virtual Network**, **IKE Alg** (Internet Key Exchange Application Level Gateway), **Tx(Byte)** (transmitted data in bytes), **Rx(Byte)** (received data in bytes), and **Uptime** (the amount of time that the network is running).

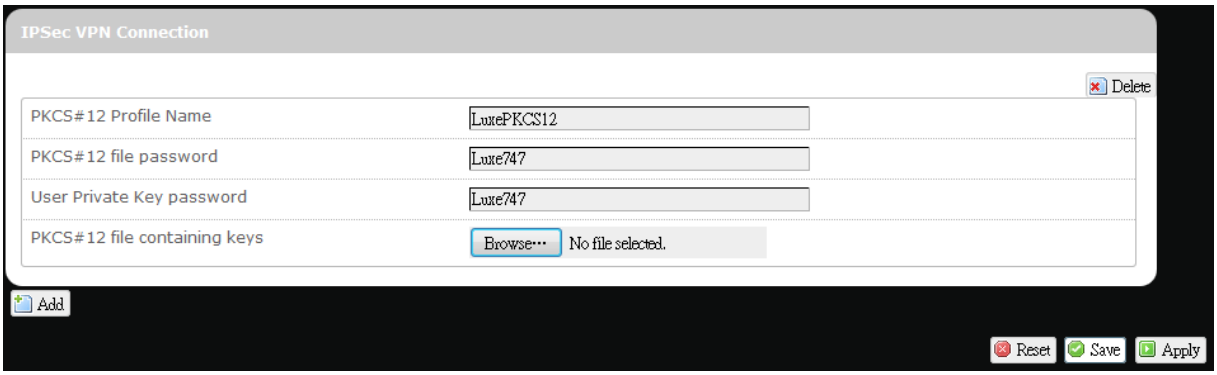
IPSec Certificate



IPSec VPN Connection

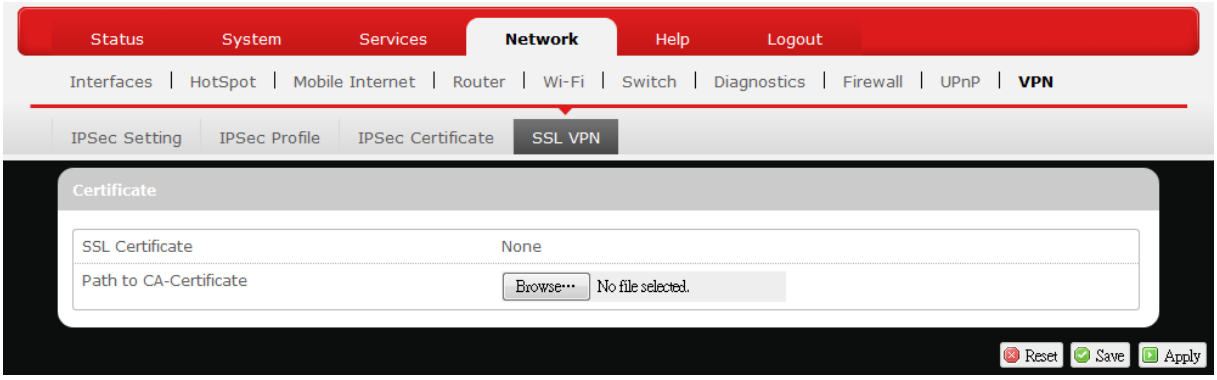
This setting allows you to use an IPSec Certificate for the VPN connection.

To setup an IPSec VPN Connection:



1. **PKCS#12 Profile Name**: Enter the profile name for the PKCS #12 certificate file to be used.
2. **PKCS#12 file password**: Enter the password for the PKCS #12 certificate file to be used.
3. **User Private Key password**: Enter the user private key password associated with the VPN connection.
4. **PKCS#12 file containing keys**: Click **Browse** and select the PKCS#12 certificate file to be used for the VPN connection.
5. To use an additional IPsec certificate, click Add and repeat Steps 1-4.
6. After making all changes, click Apply.

SSL VPN



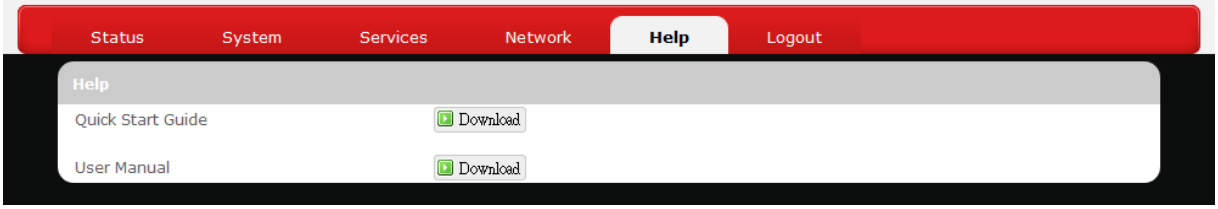
This submenu setting hosts configuration options for SSL VPN (Secure Socket Layer Virtual Private Network).

SSL Certificate: Displays SSL Certificate information.

Path to CA-Certificate: Click Browse··· and select an appropriate CA-Certificate file.

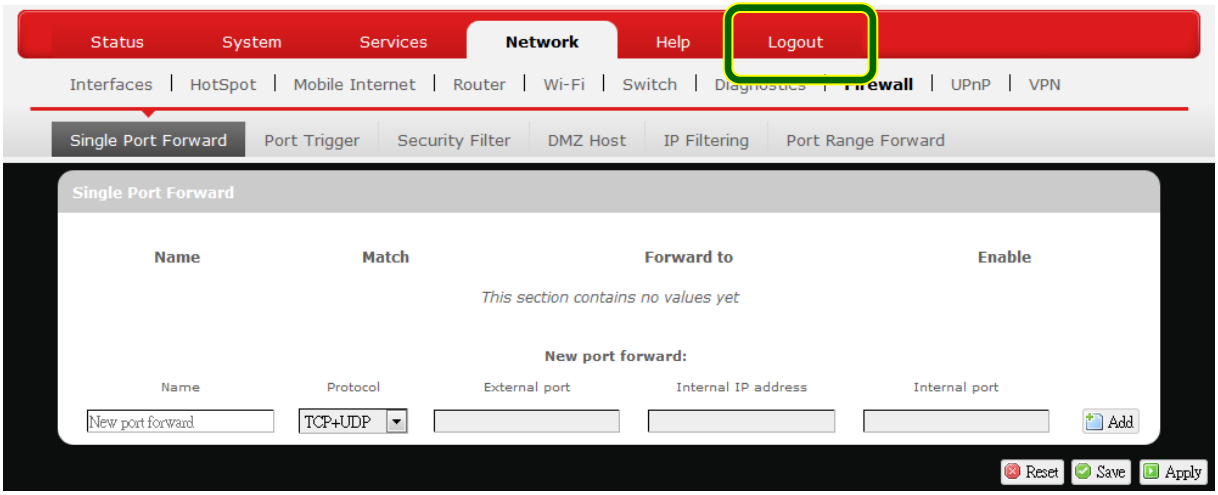
After making any changes, click Apply.

Help



Click the appropriate download link to download the latest Quick Start Guide or User Manual of this product.

Logout



Exits the web configuration interface and re-directs to login prompt.

Note:	After a period of inactivity, automatic logout will occur. After clicking any menu item, the login prompt will appear as re-login is needed to continue using the web configuration interface.

Appendix A: Installation Guide for Vehicle Usage

K530 series router is designed for rugged mobile field use that meets MIL810G military standard for drops, vibration, humidity, and extreme temperatures. To ensure proper operation of K530 series router, ***please consider below guidelines for optimal vehicle installation.***

Location and Cable wiring

- Place the router as close as possible to the voltage regulators such as power management block and filters. Keep the power cables short between device and output connectors of the voltage regulators.
- Use proper wire size according to expected current load.

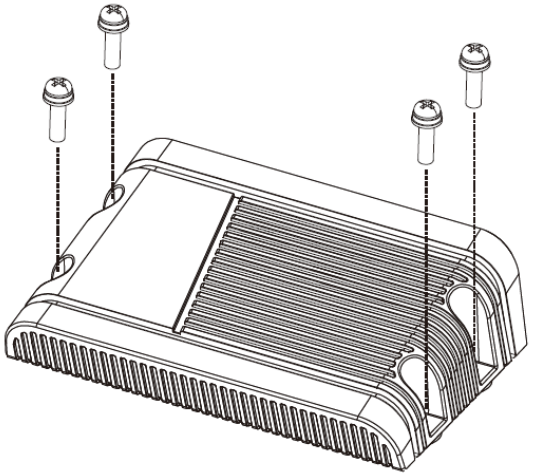
	AWG Rating	
Electric Current Load (Amps)	10-Feet Cable	20-Feet Cable
3-10	14 AWG	12 AWG
11-20	14 AWG	10 AWG
21-35	8 AWG	6 AWG

- A dedicated ground wire is highly recommended instead of direct attachment to chassis ground.
- To minimize noise interference, a filter can be applied to isolate the router from other electrical devices.

Mounting

To ensure device is securely mounted, 4 screws can be applied as shown in figure below. Choose a location to mount the device such that good ventilation and easy power supply present.

Avoid mounting the device near a spot subject to extreme heat, such as engine room or exposed to direct sunlight.



Stable Power supply

Consider below two types of voltage supply problems in a vehicle for stable power supply.

Brown-out voltage problem

The spark plug would draw significant stream of instantaneous electrical power from the car battery when starting the engine. Therefore the voltage supplied to other electrical equipment drops significantly lower than its normal level.

Transient voltage problem *(sometimes called spikes)*

The significantly changed positive or negative voltage may be caused by interference from the electrical-mechanical components in the vehicle, or even from additional electrical equipment connected to the vehicle's electrical power system. Without treatment, sharp spikes are a potential threat to K530S as well as other electrical equipment on the vehicle.

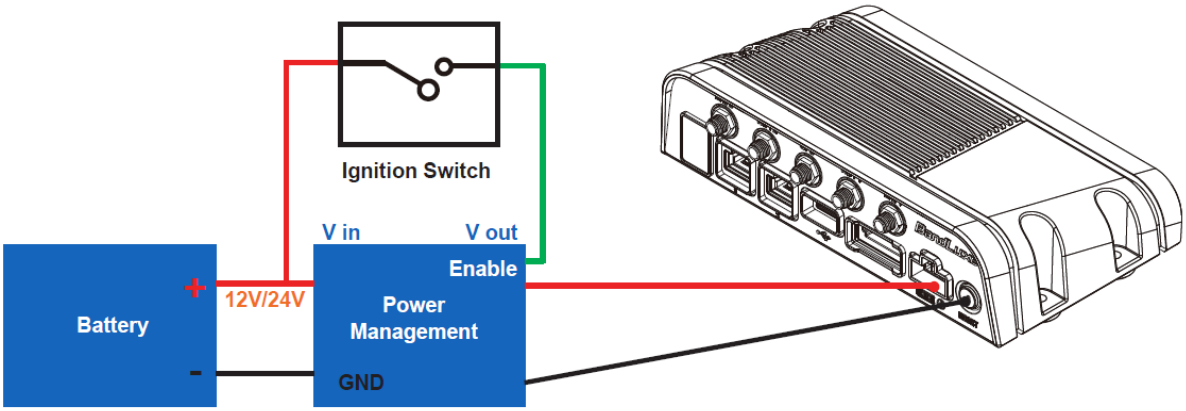
To protect device and prevent the undesirable voltage transients or brown-outs, it's required to regulate input voltage before feeding it to the power input of device.

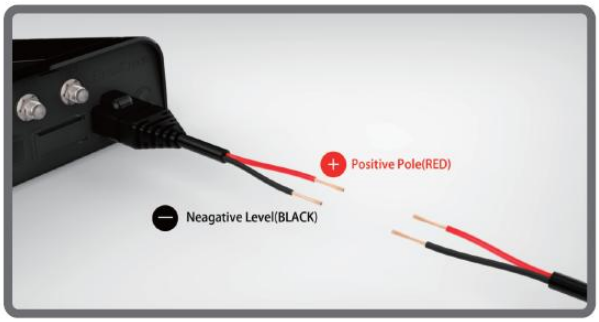
There are two ways of electrical voltage regulation. One way is to

implement a power management block that harnesses battery power during engine startup. The more effective way is to implement a power management block with filters that further smoothes out residual spikes.

Power Management

Voltage regulation is done solely on the power management block, which routes battery power to the ignition switch during engine startup, while rendering conditioned output DC power to the vehicle's electrical parts. Please see figure below for power management.

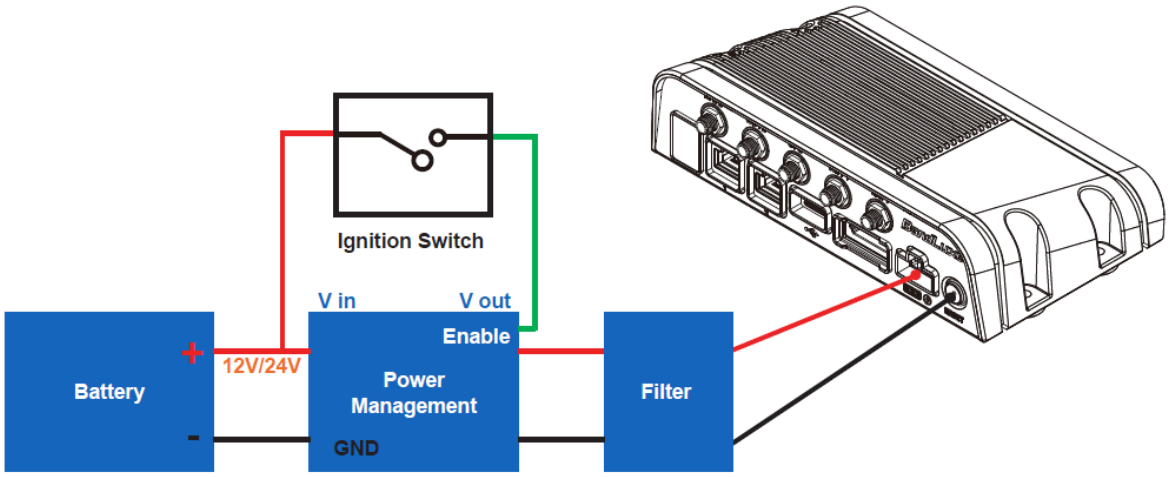


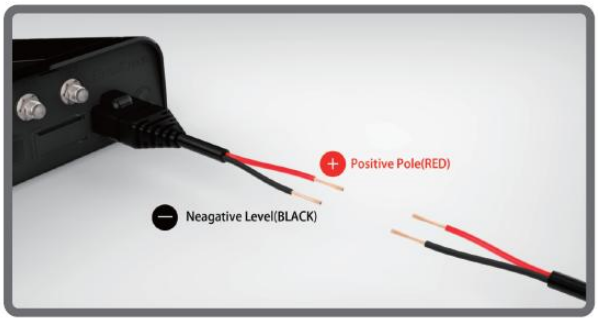


- ❖ Provide power only when ignition switch is turned on.
- ❖ Be aware of battery voltage. It is prohibited to connect to the K530 when voltage is out of operating range. (K530 operation voltage is 9~32V.)
- ❖ Do not apply power to K530S when the starter motor is engaged.
- ❖ The power management system should allow the K530S to remain powered on for a period of time after the ignition is switched off to prevent battery drain. This time is typically user programmable.

Power Management with Filter

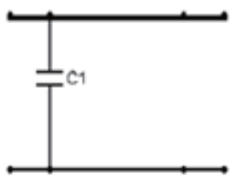
The added part further conditions power voltage with the use of a filter, which can further smooth out residual transients left over by the power management block.





There are three types of filters: capacitor, inductor, and Pi.

- The capacitor reduces transients by temporarily storing some electrical energy in the electrostatic field (electrical capacitance caused by voltage differences between two plates with the dielectric material in between) and gradually releasing them over time.

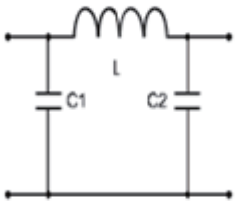


Capacitor

- The inductor reduces transients by temporarily storing some electrical energy in the magnetic field (electrical induction caused by electric currents) and gradually releasing them over time.

Inductor

- The Pi filter reduces transients by a specially designed RLC circuit, which combines both capacitors and inductors utilizing transient-reducing characteristics of both types of filters.



Pi

While any of the three types of filters will do the job, the Pi type is the optimal choice, combining advantages of both capacitor and inductor types of filters.

Appendix B: FAQ

Q: What should I know and how long does it take when I upgrade the firmware of router or modem?

A:
1. While upgrading the firmware requires some time to finish. During that, you MUST NOT turn off the power or interrupt the progress.
2. You may use an Ethernet cable or a wireless connection to upgrade the firmware. We suggest the use of an Ethernet cable.
3. It may take 2 minutes to upgrade the firmware of the router and 5 minutes to upgrade the firmware of the modem.
4. When the firmware of the modem is upgrading, the UMTS LED will flash among Blue-Green-Red. You should wait until the LED is in single color (about 4-5 minutes).

Q: How do I connect to the router?

A:
1. Connect an Ethernet cable between PC/Notebook (NB) and the router.
2. Use WiFi to connect.

Q: What's the default "User name" and "Password" for the router?

A: User name: admin
Password: admin

Q: How do I enter GUI and setup the configuration for the router?

A:
1. Connect PC/NB to the router.
2. Open Internet Explorer or other Web browser.
3. Input "http://192.168.1.1".
4. Input User name and Password.

Q: Why can't I connect to the network via built-in 3G module?

A:
1. Check the SIM/USIM to see if it is inserted well.
2. Check the UMTS LED on the router to see if it is solid.
3. Check the Status on GUI to see if the SIM/USIM detected well.
4. Check the Status on GUI to see if the APN it is correct.
5. Check the Internet on GUI to see if the Connection is "Keep Alive" or not.

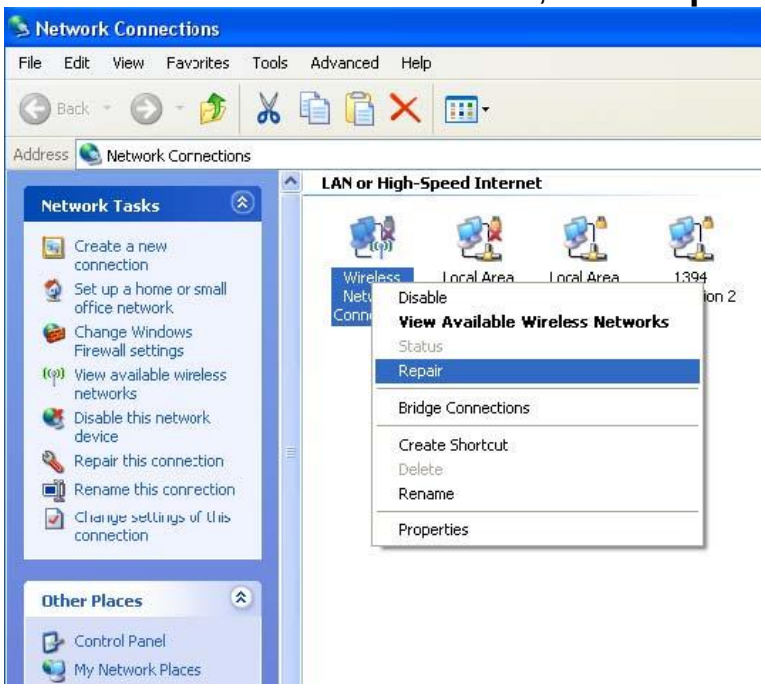
Q: Why can't I link on the GUI?

A: If you have changed your WiFi security, SSID, Local IP address, you have to repair your network to get a new IP that you can link the GUI.

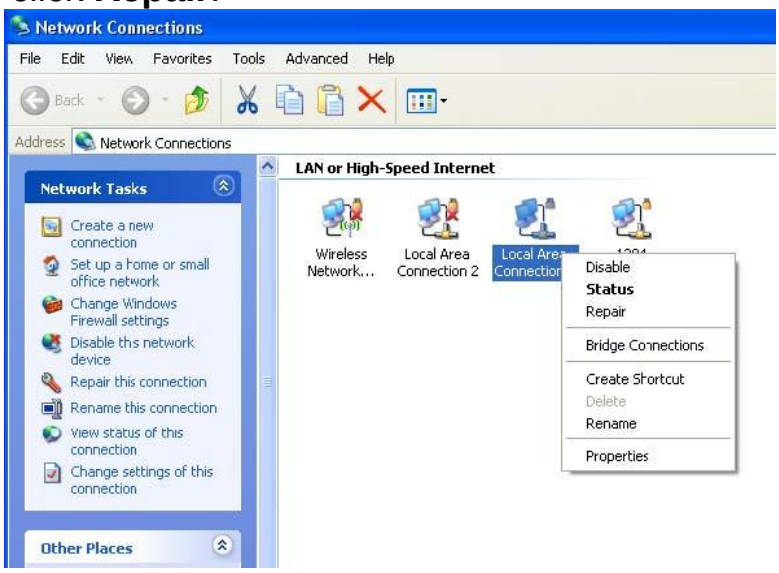
XP:

If you are a WiFi user, click **Network Connections** and right click on

Wireless Network Connection, click **Repair**.

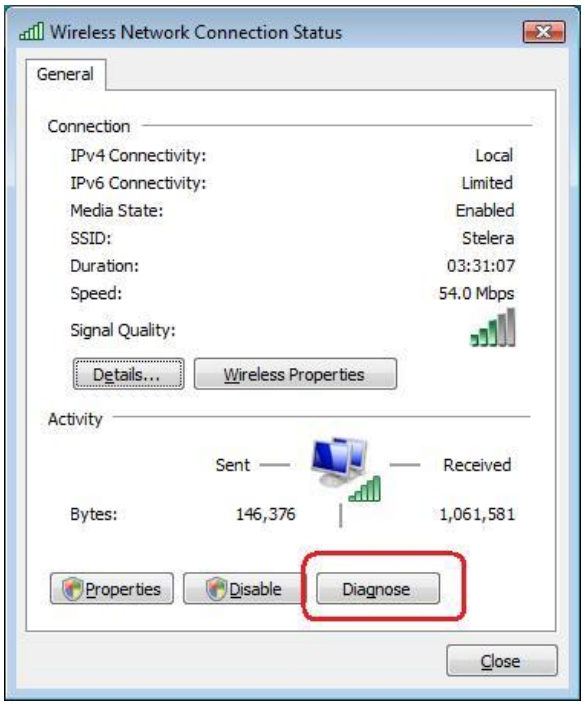


If you use Local Area Connection to connect the Router, click **Network Connections** and right click on **Local Area Connection**, click **Repair**.



Vista/7:

1. If you are a WiFi user, please click **Network and Sharing Center > Manage network connections > Wireless Network Connection > Diagnose**.



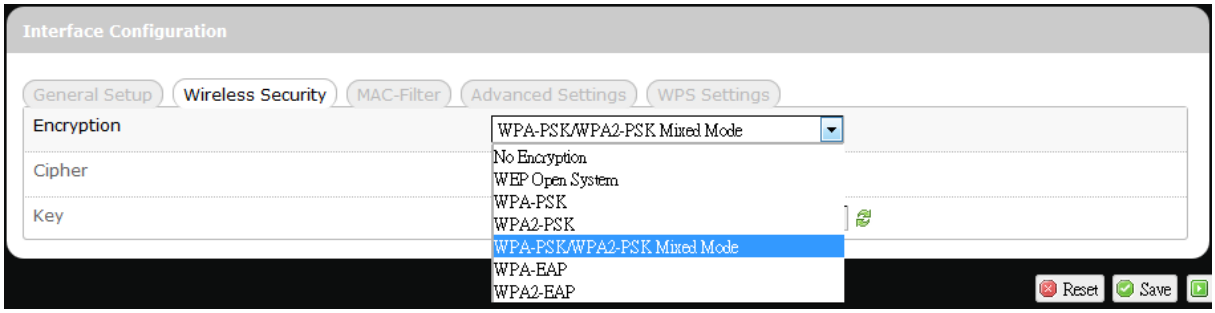
2. Please click **Reset the network adapter "Wireless Network Connection"** and it will began to repair.

Windows Network Diagnostics
Windows did not find any problems with this computer's network connection.
If you think there is still a problem, you can do one of the following:
Send a report to Microsoft.
Reset the network adapter "Wireless Network Connection"
Resetting the adapter can sometimes resolve an intermittent problem.
OK

3. If you use Local Area Connection to connect the Router, please click **Network and Sharing Center > Manage network connections > Local Area Connection > Diagnose**, follow step 1 and the subsequent messages to repair it.

Q: How do I configure my WiFi settings from GUI?

A: Click the menu tabs **Network ➔ Wi-Fi** to access to the Wi-Fi submenu, and then click the submenu tab of a particular ESSID. If you want to configure WiFi Security please click the "Wireless Security" tab under "Interface Configuration".
There are seven wireless security encryption options supported by the Router: **WEP Open System**, **WEP Shared Key**, **WPA-PSK**, **WPA2-PSK**, **WPA-PSK/WPA2-PSK Mixed Mode**, **WPA-EAP**, and **WPA2-EAP**.



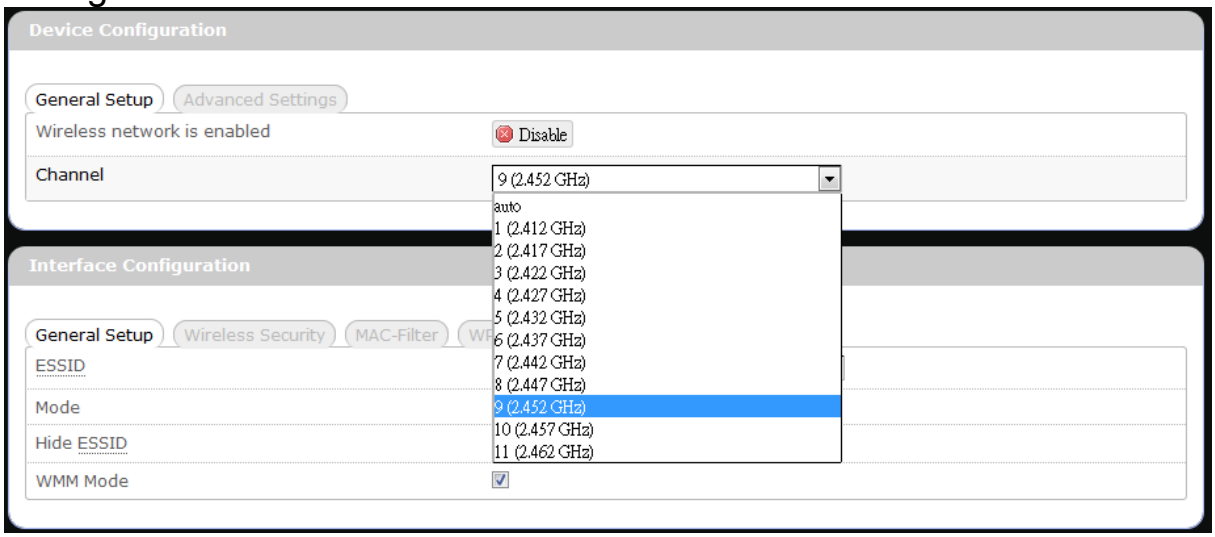
Q: Why can't I use the router in the office?
A: Your router's IP address might conflict with the office default settings.

Q: Why is my internet speed is so slow with the router?
A: 1. Click the menu tabs **Status ➔ Mobile Internet** to check the Rx Signal Strength in dBm. Weak signals will significantly slow down internet speed.

The following table is an approximate guide for signal strength.

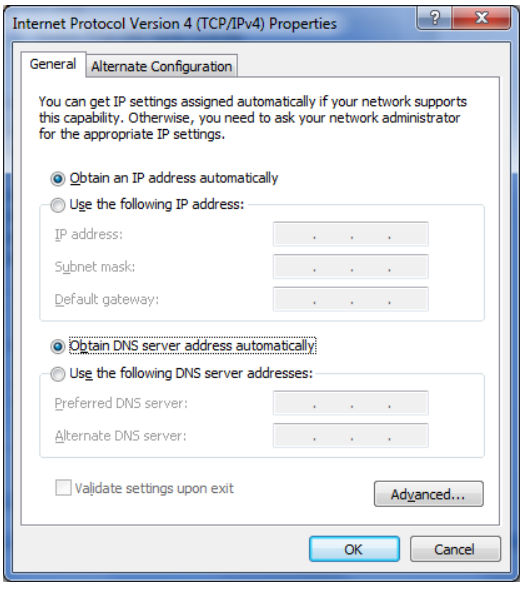
Signal Strength	**3G/2G/cdma2000 RSSI reading**	**4G LTE RSRP reading**
No signal or weak signal	Weaker than -100 dBm	Weaker than -115 dBm
Strong signal	-80 dBm or stronger	-91 dBm or stronger

2. Click the menu tabs **Network ➔ Wi-Fi** to access the Wi-Fi submenu, and then click the submenu tab of the currently used ESSID. Then select a different WiFi Channel under “Device Configuration.”



Q: I have connected the computer with the router via LAN connection. Why can’t I access the router’s IP address “http://192.168.1.1” ?

A: Your computer’s IP address and DNS server addresses may have been assigned manually. Please set your computer’s IP address and DNS server addresses to be obtained automatically. The Windows setup path is: **Control Panel ➔ All Control Panel Items ➔ Network and Sharing Center ➔ Local Area Connection ➔ Properties ➔ Internet Protocol Version 4 (TCP/IPv4))**.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Q: Why can’t I use VPN via Router?

A: You may check your office IP settings, the IP settings must not conflict with each other.

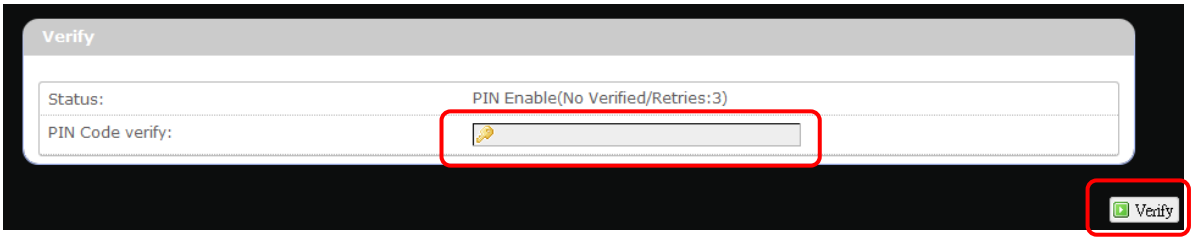
Q: Can I prevent others from using my router?

A: Yes, there are some ways to prevent others from using your router.
1. Enable your WiFi client filter.
2. Disabled your SSID Broadcast.

3. Setting your WiFi security.

Q: My PIN code is enabled and where can I input the PIN code to use my Router?

A: Click the menu tabs **Network ➔ Mobile Internet ➔ U/SIM PIN Management**; enter your PIN Code and click Verify.

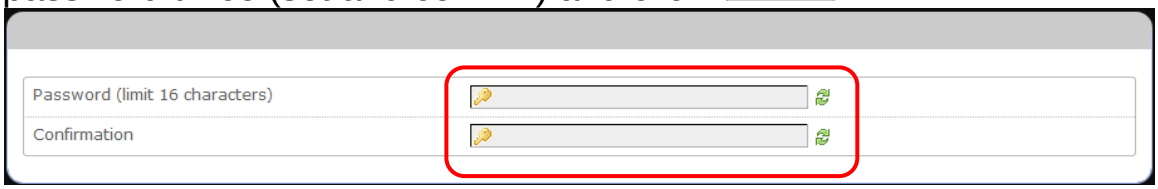


Q: Why does my U/SIM status display “PIN Disable”?

A: Check that the SIM card (which is properly activated by your mobile internet service provider) is inserted correctly in your router.

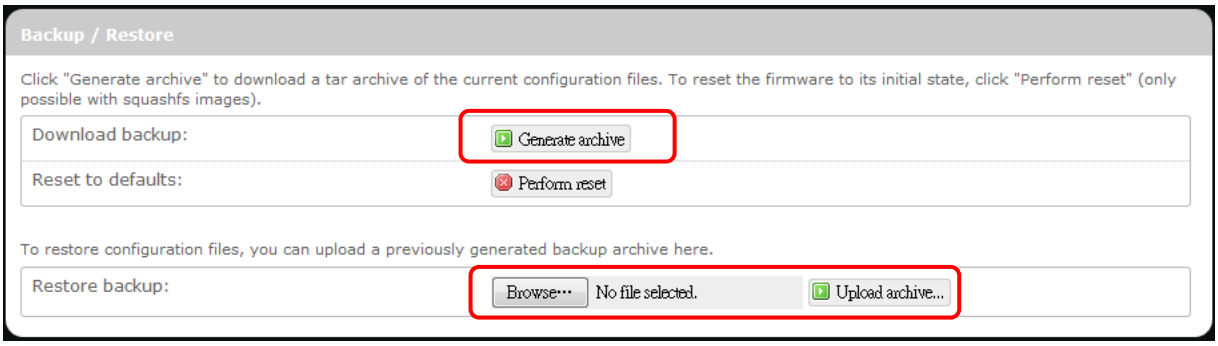
Q: Where can I change the password of the router?

A: Click the menu tabs **System ➔ Administration** . Enter the new password twice (set and confirm) and click Apply.



Q: Can I backup and restore all my settings of the router?

A: Yes. Click the menu tabs **System ➔ Backup / Flash Firmware** and click Generate archive, then follow instructions on the screen to save router settings as a TAR file at a desired location on your computer or mobile device. Conversely, to restore previously saved router settings, click Browse... (of “Restore backup”); follow screen instructions to choose the previously saved TAR file; and then click Upload archive... .


Backup / Restore
Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).
Download backup:
Generate archive
Reset to defaults:
Perform reset
To restore configuration files, you can upload a previously generated backup archive here.
Restore backup:
Browse...
No file selected.
Upload archive...

Q: How do I use the **Reset** button on the router?

A: 1. Short press the Reset button to restart the router.
2. Long press the Reset for more than 10 sec to reset the router to factory default settings.

Q: Where can I reset the router to factory default settings?

A: 1. Long press the **Reset** button on the router for more than 10 sec.
2. Click the menu tabs **System ➔ Backup / Flash Firmware** and click Perform reset.

Q: If I remove the SIM when 3G is connected, why can't I see the SIM status change?

A: You have to restart the router to see the status. It is best to remove the SIM card when the router is OFF.

Appendix C: Specifications

Note: Specifications are subject to change without notice.

Physical	
WLAN	802.11 b/g/n (2x2 MIMO)
Cellular modem	Embedded, 3GPP Rel 9, LTE FDD&TDD/eHRPD/EVDO/CDMA
Dimensions (LxWxH, mm)	160 x 94 x 44
Weight (g)	474
Interface	
Reset Button	Yes
RJ45 Ports	2 x RJ-45, 10/100 LAN ports
DC Power Jack	12V or 24V, accepting 9-32 V voltage swing
SIM slot	Embedded SIM as default, also 1 x SIM slot for external plug in for back up
USB Port	1 x USB port, for USB client device plug in only. K530S serve as USB host.
Connectivity and Data Speed	
4G LTE Band	Band 25, Band 26, Band 41
LTE Data Rate	FDD Downlink up to 100Mbps, Uplink up to 50Mbps TDD Downlink up to 68Mbps, Uplink up to 17Mbps (in configuration 3)
LTE Bandwidth	Up to 20 MHz
3G EVDO/CDMA Band	BC0, BC1, BC10
WLAN	802.11 b/g/n, 2x2 MIMO

Antenna	
Cellular embedded main antenna	No
Cellular embedded diversity antenna	No
Cellular external main antenna port	Yes SMA type
Cellular external diversity antenna port	Yes SMA type
WiFi antenna	No Embedded
WiFi external antenna port	2 x SMA ports
GPS antenna port	Yes SMA type, supporting 3.3V DC Active Antenna
Router Features	
Routing	Static Routing, Dynamic Routing (RIP, BGP, OSPF)
Security	Multiple VPN pass-through (IPSec, PPTP, L2TP), Stateless and SPI Firewall
NAT-NAPT	Single Port Forwarding, Port Range Forwarding, Port Range Triggering, Port Filtering, IP Filtering, DMZ, UPnP, Multicast Pass-Through
VPN	IPSec, SSL
DNS	DNS Agent, DDNS
Other features	IPv4 and IPv6, TCP, UDP, ICMP, ARP, DHCP Server/Client, HTTP/HTTPs, NTP, ALGs

Wireless LAN	
802.11b data rate	1/2/5.5/11 Mbps
802.11g data rate	Up to 54 Mbps
802.11n data rate	Up to 300 Mbps
Security Types	WPA/WPA2 AES/TKIP Encription, WPA/WPA2 PSK, WPA/WPA2 Enterprise, None/64/128 bits WEP Encryption, open system authentication.
Device Unique Default Encryption Key	Such unique key is linked to IMEI address of the device
Channel Selection	Auto or Manual
Other features	SSID broadcast disable, Dual SSID, Access control (MAC filtering), WLAN on/off software switch.
Status Indication	
LED Display	6 x LEDs: #1 cellular technology (Blue: LTE, Green: EVDO/CDMA, Red: SIM error or service failure) #2 signal strength (tri-color) #3 LAN 1 #4 LAN 2 #5 GPS #6 WiFi
Software Features	
Web Graphic User Interface (GUI)	Yes, Browser supported: IE, Firefox, Safari, Chrome
Web Graphic User Interface (GUI) Language Support	English
Connection Status in Web Graphic User Interface (GUI)	Network name, Signal strength, Roaming indication, Radio technology, Connection status, Connection time, Connection Statistics.
Connection management	Connection on demand, Connection when available, Auto APN matching with USIM , APN database update through browser-based Graphic User Interface (GUI), APN profile, PIN management, Preferred radio NW type selection

System protection	Password protected administrator and user access authority (provisioning, configuration, authentication).
GNSS	Supports GPS and Glonass composite location data for remote server and local access
Support FW version upgrade	Yes
Device Management	TR-069, OMA-DM, Remote Graphic User Interface (GUI) Log-in
Accessories	
Power Adapter	Input: 100to240V, 50to60Hz AC; Output: 12V DC
Environment	
Operation Temperature	-20°C to 70°C (-4°F to 158°F)
Storage Temperature	-40°C to 80°C (-40°F to 185°F)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Certification & Conformance	
	RoHS, IP64, MIL 810-G, FCC, Sprint Certification

Appendix D: Important Safety Information and Glossary

Europe – EU Declaration of Conformity

CE

European Union Notice
Products with CE marking comply with the R&TTE Directive (99/5/EC), the EMC Directive (2004/108/EC), and the Low Voltage Directive (2006/95/EC) issued by the Commission of the European Community.
Compliance with these directives implies conformity to the following European Norms (in parentheses are the equivalent international standards).

EN 60950-1 (IEC 60950-1)
Safety of Information Technology Equipment.

EN 300 328
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; data transmission equipment operating in the 2.4 GHz ISM band and using spread spectrum modulation techniques.

EN 301 489-24
Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 24: Specific conditions for IMT-2000 CDMA direct spread (UTRA) for mobile and portable (UE) radio and ancillary equipment.

ETSI EN 301 511
Global system for mobile communications (GSM); Harmonised EN for mobile stations in the GSM 900 and GSM 1800 bands, covering essential requirements of article 3.2 of the R&TTE directive (1995/5/EC).

ETSI EN 301 489-1
Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements.

ETSI EN 301 489-7
Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS).

ETSI EN 301 489-17
Electromagnetic compatibility and Radio spectrum Matters (ERM);
Electromagnetic Compatibility (EMC) standard for radio equipment and services;
Part 17: Specific conditions for 2.4 GHz wideband transmission systems.

ETSI EN 301 908-1 & -2
Electromagnetic compatibility and Radio spectrum Matters (ERM); Base Stations (BS), Repeaters and User Equipment (UE) for IMT-2000 Third Generation cellular networks;
Part 1: Harmonised EN for IMT-2000, introduction and common requirements, covering essential requirements of article 3.2 of the R&TTE Directive.

EN 50385
Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110 MHz - 40 GHz) - General public.

Federal Communication Commission Interference Statement

15.21
You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

15.105(b)

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
1) This device may not cause harmful interference and
2) This device must accept any interference received, including interference that may cause undesired operation of the device.

FCC RF Radiation Exposure Statement:
For body worn operation, this device has been tested and meets FCC RF exposure guidelines when used with an accessory that contains no metal and that positions the device a minimum of 20 cm from the body. Use of other accessories may not ensure compliance with FCC RF exposure guidelines.

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Glossary

2G: Second-generation mobile networking technology. Represents a switchover from analog to digital; most 2G networks use GSM.

3G: Third-generation mobile networking technology that enables simultaneous transfer of voice and non-voice data; most 3G networks use WCDMA.

3.5G: A more recent standard of mobile networking technology; generally uses HSDPA.

3.75G: A more recent standard of mobile networking technology; generally uses HSUPA.

4G: A more recent standard of mobile networking technology; generally uses LTE.

APN (Access Point Name/Network): Provides GPRS routing information. Consists of:

Network ID: Identifies the external service requested by a GPRS user.

Mobile network operator ID: Specifies routing information.

ARFCN (Absolute Radio Frequency Channel Number): The specific ID numbers for all radio channels used in cellular mobile communications.

bps (bits per second): How data flow is measured.

CHAP (Challenge Handshake Authentication Protocol): CHAP identifiers are changed frequently and authentication can be requested by the server at any time.

DNS (Domain Name System): Helps route network traffic by making the addressing process more user-friendly.

DHCP (Dynamic Host Configuration Protocol): How devices obtain IP addresses from a server.

DUN (Dial-Up Network): Windows component that enables online access via a modem.

EDGE (Enhanced Data GSM Environment/Enhanced Data for Global Evolution): Advanced GPRS that delivers multimedia and other data needing greater bandwidth at up to 237 kbps.

eHRPD (Evolved High Rate Packet Data): An upgrade of the existing *HRPD (High Rate Packet Data)* and EV-DO (Evolution-data Optimized) network technology to allow smooth transitioning from 3G mobile network technology to 4G LTE network technology.

GPRS (General Packet Radio Service): Delivers data in packets at up to 86 kbps.

GSM (Global System for Mobile Communications): The most popular cellular network, mostly operates in 850-900 or 1800-1900 MHz; the primary 2G system.

HSDPA (High Speed Downlink Packet Access): Advanced WCDMA that delivers downlink bandwidth intensive data at up to 7.2Mbps; typically associated with 3.5G.

HSUPA (High Speed Uplink Packet Access): Advanced WCDMA that delivers uplink bandwidth intensive data at up to 5.76Mbps; typically associated with 3.75G.

HSPA+ (High Speed Packet Access +): This is also known as HSPA Evolved, is the next step and is more focused on delivering data services enabling speeds of up to 42Mbps in the downlink and 11Mbps in the uplink.

IMEI (International Mobile Equipment Identity): A number unique to each GSM/UMTS device that can be used block network access by a stolen mobile device.

IP (Internet Protocol): Routes packets over a network.

IPSec (Internet Protocol Security): Security implementation of IP communications by authenticating and encrypting each IP packet during network communication.

Kbps (Kilobits per second): A data flow measure; 1024 bits/second.

LAN (Local Area Network): A data network with limited range but good bandwidth.

Load Balance: A method for distributing network loads across different networks to optimize network traffic flow and increase network reliability.

LTE (Long Term Evolution): High-speed mobile communication standard based on the GSM/EDGE and UMTS/HSPA network technologies. LTE provides downlink peak rates up to 300 Mbit/s and uplink peak rates up to 75 Mbit/s.

Mbps (Megabits per second): A data flow measure; 1,048,576 bits/second.

MDN (Mobile Directory Number): The telephone number of the mobile device. In other words, it is the directory number that is assigned to a mobile subscriber.

MSID (Mobile Station Identification): The identification number for the mobile station. The *MSID* can be a *MIN (Mobile Identification Number)* or *IMSI (International Mobile Subscriber Identity)*.

MSL (Maximum Segment Lifetime): The maximum amount of time (arbitrarily defined as 2 minutes) that a TCP segment can exist in the internetwork system.

PAP (Password Authentication Protocol): The difference between PAP authentication and a manual or scripted login, is that PAP is not interactive. The username and password are entered in the client's dialing software and sent as one data package as soon as the modems have established a connection, rather than the server sending a login prompt and waiting for a response.

PPP (Point-to-Point Protocol): An internet connection method.

PIN (Personal Identity Number): Four to eight digital numbers SIM card security code; allows access to the carrier’s network.

Rx: Shorthand for Reception.

SIM (Subscriber Identity Module): A small card that contains key mobile device identification, subscription and contact information.

Tx: Shorthand for Transmission.

WCDMA (Wideband Code Division Multiple Access): Advanced EDGE that supports 384kbps data flow. Most 3G networks use this standard, the same as UMTS.

UAM (Universal Access Method): A method to allow WiFi access to a wireless network while roaming. Using a regular web browser, the roaming customer enters a login page and provides user information (usually username and password) to access the network.